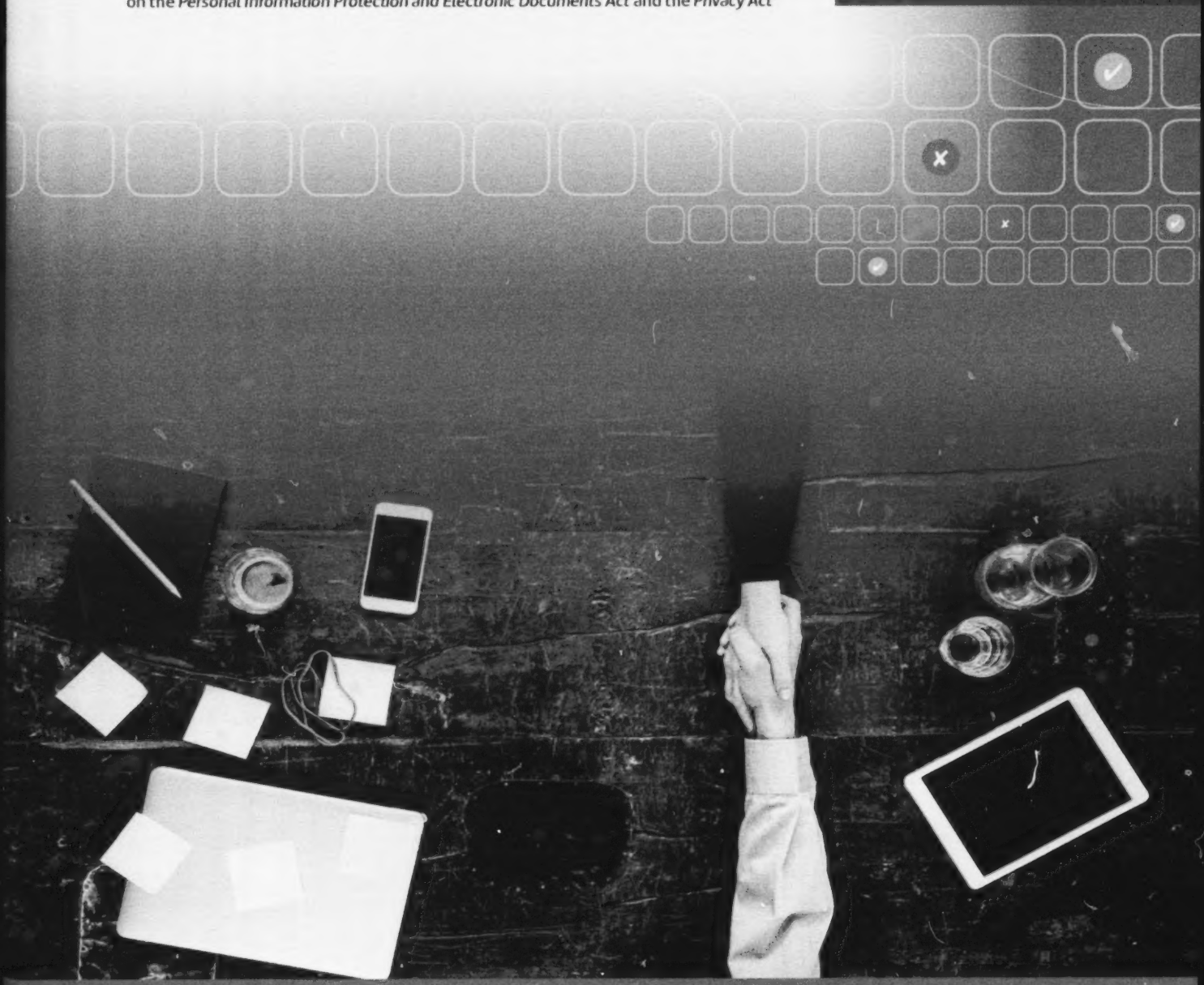
Office of the
Privacy Commissioner
of Canada

2017–18 Annual Report to Parliament

on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*



TRUST BUT **VERIFY**

Rebuilding trust in the digital economy
through effective, independent oversight

2017-18 Annual Report to Parliament on the
Personal Information Protection and Electronic Documents Act and the *Privacy Act*

Trust but verify
Rebuilding trust in the digital economy through effective, independent oversight

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, QC K1A 1H3

© Her Majesty the Queen of Canada for the Office of the Privacy Commissioner of Canada, 2018
Cat. No.: IP51-1E-PDF
ISSN: 1913-3367

Follow us on Twitter: @PrivacyPrivee
Facebook: https://www.facebook.com/PrivCanada/

Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
1 800 282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec)
K1A [illegible]
Tél. : [illegible]5444
1 800 282-1376
www.priv.gc.ca

The Honourable George J. Furey, Senator
The Speaker
Senate of Canada
Ottawa, Ontario K1A 0A4

September 2018

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada, for the period from April 1, 2017 to March 31, 2018. This tabling is done pursuant to sections 38 for the *Privacy Act* and 25 for the *Personal Information Protection and Electronic Documents Act*.

Sincerely,
Original signed by

Daniel Therrien
Commissioner

Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
1-800-282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (819) 994-5444
1-800-282-1376
www.priv.gc.ca

The Honourable Geoff Regan, M.P.
The Speaker
House of Commons
Ottawa, Ontario K1A 0A4

September 2018

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada, for the period from April 1, 2017 to March 31, 2018. This tabling is done pursuant to sections 38 for the *Privacy Act* and 25 for the *Personal Information Protection and Electronic Documents Act*.

Sincerely,

Original signed by

Daniel Therrien
Commissioner

Table of Contents

Commissioner's message 1
- The Facebook/Cambridge Analytica crisis 1
- Progress from government slow to non-existent 2
- Guidelines on meaningful consent and inappropriate practices 3
- Reputation 4
- A proactive vision for privacy protection 5
- Final thoughts 7

Privacy by the numbers 9

The *Personal Information Protection and Electronic Documents Act* – A year in review 11
- Consent and control 11
- PIPEDA investigations in general 22
- Parliamentary activities related to PIPEDA 29
- Contributions Program 33

The *Privacy Act* – A year in review 35
- National security 35
- Privacy at the border 36
- *Privacy Act* reform and parliamentary activities 38
- *Privacy Act* investigations 40
- Advice to government 51

Privacy cases in the courts 61
- Cases in which the Office was a participant this past year 61
- Cases we followed with interest 63

International and domestic cooperation 65
- International Conference of Data Protection and Privacy Commissioners 65
- Asia Pacific Privacy Authorities 66
- Global Privacy Enforcement Network (GPEN) 66
- Canadian Anti-spam Law (CASL) 66
- Federal-provincial-territorial cooperation 67
- S57 proactive engagement 67

Appendix 1 – Definitions 69

Appendix 2 – Statistical tables 72
- Statistical tables related to PIPEDA 72
- Statistical tables related to the *Privacy Act* 79

Appendix 3 – Investigation processes 92
- PIPEDA investigation process 92
- *Privacy Act* investigation process 94

Appendix 4 – Report of the Privacy Commissioner, Ad Hoc, for 2017-18 96

Commissioner's message

The Facebook/Cambridge Analytica crisis

Sometimes it takes a crisis to effect change and this past year has seen no shortage of privacy crises.

There were the unfortunately familiar data breaches, affecting millions of customers of companies like Equifax, Uber and Nissan Canada Finance, to name a few. And there was of course the Facebook/Cambridge Analytica matter, which we are now investigating, widely seen as a serious wake-up call that highlighted a growing crisis for privacy rights.

With the Facebook matter, individuals must now confront the idea that personal information may be analyzed for far more insidious purposes than marketing. In this instance, the allegations are that our information was used to influence political opinions. What next? How else are we being manipulated?

These issues also underscore deficiencies in Canada's privacy laws that I and my predecessors have tried to draw attention to for years. This past year alone, we've had numerous opportunities to highlight those deficiencies and propose potential solutions.

We have testified and made submissions to parliamentarians on the need to modernize the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and proposed changes to national security legislation, Bill C-59, in which we reiterated a number of the recommendations we made on *Privacy Act* reform in 2016, among other things.

We also drew attention to the lack of standards and oversight over the personal information handling practices of political parties. The government introduced legislation intended to respond to this important gap.

Bill C-76, however, adds nothing of substance in terms of privacy protection. Rather than impose internationally recognized standards, the bill leaves it to parties to define the rules they want to apply. It does not impose independent oversight. On this and many other fronts, Canada's privacy legislation is sadly falling behind what is the norm in other countries.

Canadians want to enjoy the many benefits of the digital economy, but they rightly expect they can do so without fear

that their rights will be violated and their personal information will be used against them. They want to trust that rules, legislation and government will protect them from harm.

The time of self-regulation is over. In Canada we, of course, have privacy legislation but it is quite permissive and gives companies wide latitude to use personal information for their own benefit. Under PIPEDA, organizations have a legal obligation to be accountable, but Canadians cannot rely exclusively on companies to manage their information responsibly. Transparency and accountability are necessary but they are not sufficient.

To be clear, it is not enough to ask companies to live up to their responsibilities. Canadians need stronger privacy laws that will protect them when organizations fail to do so. Respect for those laws must be enforced by a regulator, independent from industry and the government, with sufficient powers to ensure compliance.

Trust but verify. In order to increase trust in the digital economy, we must ensure that Canadians are able to count on an independent third party who can verify compliance with privacy laws.

Given the opaqueness of business models and the complexity of information flows in the age of data analytics, artificial intelligence (AI) and the Internet of Things, that regulator, my Office federally, should be authorized to inspect the practices of organizations even if a violation of law is not immediately suspected. Individuals are unlikely to file a complaint when they are unaware of a practice that may harm them.

In other words, trust but verify. In order to increase trust in the digital economy, we must ensure that Canadians are able to count on an independent third party who can verify compliance with privacy laws.

We have also asked Parliament to study the issue of de-indexing and source takedown with a view to confirming the right balance between the right to reputation and privacy, freedom of expression and public interest.

On the public sector side, we have proposed amendments to Bill C-59 that strike a better balance between national security and respect for basic individual rights, including the right to privacy.

Progress from government slow to non-existent

Several parliamentarians have supported our call for legislative reform. Notably, in February, 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), which is tasked with reviewing Canada's privacy laws, concurred with many of our recommendations to amend PIPEDA, and even called for additional measures inspired by the European Union's General Data Protection Regulation (GDPR), which came into force in May.

In a later report in June, after hearing from witnesses on the Facebook/Cambridge Analytica matter, ETHI came to the view that some amendments (notably those conferring new enforcement powers to my Office, including the power to inspect or audit) were urgently required. ETHI also agreed that political parties need to be governed by privacy laws.

Unfortunately, progress from government has been slow to non-existent. The only clear support was for a majority of the amendments we suggested to Bill C-59, the anti-terrorism bill. As regards the *Privacy Act*, adopted 35 years ago to regulate privacy in the public sector, the Minister of Justice announced in 2016 that she had instructed her officials to begin concentrated work towards modernizing the law – an exercise she agreed was long overdue. Yet no concrete proposal has yet been made public.

In late June 2018, the government responded to ETHI's recommendations to amend PIPEDA. The Minister of Innovation, Science and Economic Development agreed that changes are required to our privacy regime, but he argued that further study of the viability of all options, for instance on enforcement models, was required with a view to presenting Canadians with proposals. The minister launched a national digital and data consultation, which could eventually result in amendments to the law in several years.

Canadians cannot afford to wait several years until known deficiencies in privacy laws are fixed. Technology is evolving extremely rapidly and many new technologies disrupt not only business models but also social and legal norms. Legal protections must improve apace if consumer trust is to reach the level everyone desires. As ETHI commented in its June report, "the urgency of the matter cannot be overstated."

We are of course not asserting that we have reached a stage where all privacy risks are known and all solutions have been identified. There is therefore merit in the consultations announced by the government. However, several deficiencies in the law have been identified for some time, including the issue of necessary powers for the Office of the Privacy Commissioner (OPC).

We know Canadians want this and we know organizations generally would prefer not being subject to inspections, orders and fines. There is no need to consult on this issue. Now is the time to act.

While we were disappointed with the government's response, we did not wait for government to act and have undertaken a number of initiatives in areas where we do have some control. However, these were in the form of guidance, not law, and the protection they offer to Canadians is therefore limited.

Guidelines on meaningful consent and inappropriate practices

Last year in our Annual Report, we concluded that consent should continue to play a prominent role in the 21st century, as it is central to personal autonomy. Consent has an important place in privacy protection, where it can be meaningfully given with sufficient information.

Where consent may not be practicable, for instance in certain situations involving AI where data may be used for multiple purposes not always known when it is collected, other forms of privacy protection may be required. We also concluded that in all situations, additional support mechanisms are needed. This includes independent regulators that can guide industry, hold it accountable, inform citizens and meaningfully sanction inappropriate conduct.

To more effectively guide industry and help individuals in exercising their privacy rights, in May 2018, we published two important guidance documents on obtaining meaningful consent and inappropriate data practices. They marked the culmination of an extensive consultation process, which included an opportunity for stakeholders to provide feedback on draft versions released in the fall.

The consent guidance sets out advice for organizations to ensure they obtain meaningful consent. It describes seven guiding principles, including the need to emphasize four key elements in privacy notices:

- what information is being collected;
- with whom is it being shared;
- for what purposes is it being collected, used or disclosed, and
- meaningful residual risk of significant harm.

The guidance on inappropriate practices outlines for companies which practices are inappropriate and

informs individuals about what organizations are generally prohibited from doing, even with consent. This includes:

- profiling that leads to discriminatory treatment contrary to human rights law;
- collecting, using or disclosing personal information for purposes that are known or likely to cause significant harm to the individual, or
- posting personal information with the intent of charging a fee for its removal.

Our *Obtaining meaningful consent* guidance was a joint effort with our counterparts in Alberta and British Columbia and will apply as of January 1, 2019, as we want to give organizations time to implement changes to their systems and practices. Our *Inappropriate data practices* guidelines became applicable as of July 2018.

Generally speaking, the documents set out a combination of legal requirements and best practices that detail our expectations regarding what compliance entails. Once these guidelines are in application, it will be through this lens that our Office conducts its work.

I know some stakeholders were concerned about binding language in the guidance. While it is clear that we cannot use guidance to establish new legal standards, we think our role as a regulator includes giving guidance that clarifies broadly framed PIPEDA principles and sets expectations as to how the law should generally be interpreted and applied.

Given that PIPEDA is so broad in its formulation, individuals and organizations need an adequate level of certainty as to what compliance entails. It is troubling that some organizations have signaled an interest in challenging the legality of this approach. This is another reason why legislative reform is required, since having the authority to make orders would go a long way to addressing such challenges. We note that in his response to ETHI, the Minister of ISED acknowledged that "more specific guidelines or regulations may need to be articulated" to clarify PIPEDA principles "for new or emerging business models or products."

Read more about how stakeholder feedback was incorporated into the final versions of the guidance documents.

Reputation

In January, my Office released the results of a public consultation related to important questions around online reputation and privacy.

We approached this work with one key goal in mind: helping to create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.

The nature of information has changed dramatically in the digital age, creating new risks to the reputation of individuals. Social media and search engines make it much easier to have access to information. Information about us is readily available to potentially millions of people – and that information may be inaccurate, years out of date, or presented out of context.

And yet, key decisions are made about us based on searches done on social media platforms or using search engines– for example, decisions related to employment, housing or credit. So, there are real consequences.

This raises questions: as a society, do we believe reputation deserves protection against the new risks posed by the online realm? And, if yes, what form should it take?

We examined various mechanisms aimed at providing individuals with some measure of control over their online information. We looked for options that would respect the balance between privacy and other critical rights, such as freedom of expression and freedom of the press.

We ultimately came to the conclusion that the most appropriate way forward was to interpret PIPEDA in a way that protects people's online reputation. We believe that under the existing law, Canadians have a right to ask search engines to de-index web pages, and websites to remove or amend content, that contains inaccurate, incomplete or outdated information.

Our draft position on online reputation also highlighted the need to educate young Canadians in order to help develop responsible, informed online citizens.

In the months following the publication of that draft position paper, we further consulted with stakeholders.

In the meantime, our Office received complaints from individuals about Google search results. In response, Google took the position that PIPEDA did not apply to its search engine and that, in the alternative, de-indexing would be unconstitutional if the Act did apply. We therefore plan to file a reference with the Federal Court to first seek clarity on the issue of whether Google's search engine is subject to PIPEDA before proceeding further with the complaints.

We also called on the government to amend the law to effectively protect reputation in an increasingly online world. We are glad that the government, in its response to ETHI's February report, agreed it will be necessary to provide further certainty on how the Act applies in the various contexts where personal reputation may be harmed.

A proactive vision for privacy protection

It has become increasingly clear to me that to have a greater impact on the privacy rights of more Canadians, we need to change our approach as a regulator.

To that end, we have made significant changes to our organizational structure that we believe will help us achieve better results for privacy.

We have streamlined our operations by clarifying program functions and reporting relationships, and become more forward-looking by shifting the balance of our activities towards greater pro-active efforts. Our objective is to have a broader and more positive impact on the privacy rights of a greater number of Canadians, which is not always possible when focusing most of our attention on the investigation of individual complaints.

With that in mind, our work now falls into one of two program areas: promotion or compliance. Activities aimed at bringing departments and organizations *towards* compliance with the law fall under the Promotion Program, while those related to addressing *existing* compliance issues fall under the Compliance Program.

It has become increasingly clear to me that to have a greater impact on the privacy rights of more Canadians, we need to change our approach as a regulator.

While we continue to seek stronger enforcement powers, we believe that a successful regulator does not rely first on enforcement, but rather only when needed. Thus our first strategy is under the Promotion Program to inform Canadians of their rights and how to exercise them, and to guide and engage with organizations on how to comply with their privacy obligations.

Guidance and information will be issued on most key privacy issues, starting with how to achieve meaningful consent in today's complex digital environment and inappropriate data practices as mentioned earlier.

We also wish to work with industry proactively and collaboratively in an advisory capacity, to the extent our limited resources allow. We want to better understand the privacy impacts of new technologies and provide practical advice on how to use them in a privacy compliant way.

For example, we announced in May 2018 our first advisory project involving Sidewalk Toronto, a smart-city endeavor between Waterfront Toronto and Sidewalk Labs, owned by Google's parent company Alphabet. The initiative involves building a technology-driven neighbourhood on the city's eastern waterfront that includes sensors aimed at helping city planners find efficiencies.

Understandably, it is raising many questions about data collection, privacy, where the information will be stored and how it might be used.

Along with colleagues from the Office of the Information and Privacy Commissioner of Ontario, members of our Business Advisory Directorate met with those behind the project to learn more about it and how they were addressing some of these privacy concerns.

We also reminded officials of key privacy principles, including identifying the purposes for collection, obtaining consent, ensuring individuals could access their own personal information and being accountable for protecting the data and being clear about who owns it.

Overall, we are encouraged by Sidewalk Toronto's efforts to proactively address privacy and data security in the design and implementation of the initiative. Given the project is still in its early stages, we are continuing to monitor developments and proactively engage with Sidewalk Toronto officials as it progresses. We also hope the advice we provide will be helpful as other smart city initiatives pop up across the country.

Addressing privacy issues upfront and resolving matters cooperatively, outside formal enforcement, is our preferred approach. It avoids time-consuming and costly investigations, helps mitigate against future privacy risks, offers organizations a measure of consistency and predictability in their dealings with our Office and allows everyone to benefit from innovation.

It is for these reasons that we will primarily consider our promotion tools before engaging our second strategy – proactive enforcement.

Under the Compliance Program, our proactive enforcement actions will target systemic, chronic or sector-specific privacy issues that aren't being addressed through our complaint system and that we believe may inflict significant damage to the privacy rights of Canadians.

For example, we launched our first proactive, Commissioner-initiated investigation under our Compliance Program in May 2018 into the practices of six different data and list brokers.

As part of the investigation, we're looking at accountability, openness and transparency in the management of personal information and considering the means of consent obtained for the personal information collected, used or disclosed. We believe this industry can benefit from an investigation of this nature, and that Canadian consumers will welcome it.

By delineating our activities more clearly under two programs, Compliance and Promotion, by being more proactive and by ensuring we are citizen-focused, I hope Canadians may begin to feel more empowered and in control of their personal information – and generally safer in the knowledge that their rights will be respected.

Our Government Advisory Directorate is also in the business of providing advice, in this case, to federal institutions, which we've committed to doing more frequently. We wish to engage with government stakeholders earlier in the development of programs and activities so that Canadians may enjoy the benefits of innovation without undue risk to their privacy. To that end, we will enhance our guidance related to Privacy Impact Assessments (PIAs) and make it easier for institutions to prepare them.

Of course, the extent to which we can execute our proactive agenda hinges on resources. We have gone

to great lengths to find efficiencies and make optimal use of existing resources and tools. Nevertheless, we find ourselves unable to keep pace with the challenges of an increasingly complex digital environment, in no small part because Canada's privacy laws are not adapted to the realities of the 21st century.

We've requested a modest increase in permanent funding to provide interim relief pending much needed legislative reform. If received, these funds would help:

- establish a limited proactive agenda that includes arming organizations with more policy guidance on emerging issues and educating Canadians so they may take control of their privacy;
- deal with mandatory breach reporting which comes into force in November without any associated funding and, as was the case in other jurisdictions, is expected to significantly increase our workload; and
- assist our overwhelmed investigators in more expediently addressing complaints filed by concerned Canadians and proactively investigating systemic, chronic or sector specific privacy issues.

Following the Facebook/Cambridge Analytica matter, we were asked by ETHI what resources and tools my Office might need to assist in ensuring that "tech giants" and other companies truly respect their privacy obligations.

While our modest ask for increased funding would have an interesting but limited impact, a significantly larger budget might be required to actually have a true impact in terms of protecting Canadians' privacy rights, as envisaged by ETHI. This was the conclusion reached by the U.K. government recently, which decided to double the resources available to my counterpart, the Information Commissioner's Office. This would equip the OPC with a full suite of properly resourced promotion and compliance tools.

Complete funding would provide for a full set of guidance documents and ensure that they remain current, which is essential when technological leaps result in the creation of new privacy risks every day.

It would allow us to provide advice to more organizations that wish to use new technologies in a privacy compliant way. We have already experienced a great deal of interest in our Office providing more advisory services to business; right now, however, our limited advisory program would not come close to meeting such expressed demand.

In focusing on improving citizen control of their privacy, we could use innovative means such as contextual advertising to bring individuals to our site when they are about to make a decision on whether to disclose their personal information.

We would also develop effective strategies with regulators in other fields to ensure companies comply with all applicable laws, which sometimes overlap. And finally, full funding would allow the OPC to be both proactive in investigating opaque privacy practices involving risk, and responsive in a timely way to all complaints, thus achieving a greater scope of compliance amongst public and private institutions.

Recent events underscore the significant risks facing privacy protection in the digital age. Modern laws consistent with evolving international norms are urgently required if we are to provide Canadians with the protection they expect and deserve.

Final thoughts

To sum up, recent events underscore the significant risks facing privacy protection in the digital age. Modern laws consistent with evolving international norms are urgently required if we are to provide Canadians with the protection they expect and deserve.

We have undertaken several initiatives that are within our powers to enhance this protection, but to be truly effective as a regulator, we need new powers and resources.

ETHI's Vice-Chair, Nathaniel Erskine-Smith, introduced a private member's bill in June that would empower my Office to conduct audits, make orders and refer cases involving willful or reckless violations of the law for prosecution, which could result in fines.

I think the time is well past due for the government to introduce legislation along the same lines, albeit amended in such a way as to levy administrative monetary penalties rather than rely on the criminal law. I note that these proposed new powers received all-party support within the ETHI committee.

In addition, we ask the government to increase our resources so that, pending the conclusion of its consultation on a data strategy and broader legislation, my Office has the necessary tools to adequately protect the privacy of Canadians.

Privacy by the numbers

297	PIPEDA complaints accepted*
205	PIPEDA complaints closed through early resolution*
106	PIPEDA complaints closed through standard investigation*
116	PIPEDA data breach reports
1,254	*Privacy Act* complaints accepted*
441	*Privacy Act* complaints closed through early resolution*
767	*Privacy Act* complaints closed through standard investigation*
286	*Privacy Act* data breach reports
71	Privacy Impact Assessments (PIAs) received
50	Advice provided to public sector organizations following PIA review or consultation
571	Public interest disclosures by federal organizations
31	Bills and legislation reviewed for privacy implications (14 bills + 17 studies)
14	Parliamentary committee appearances on private and public sector matters
20	Formal briefs submitted to Parliament on private and public sector matters
11	Other interactions with parliamentarians or staff (for example, correspondence with MPs' or Senators' offices)
10,092	Information requests
79	Speeches and presentations
2,095,447	Visits to website
200,840	Blog visits
989	Tweets sent
13,976	Twitter followers as March 31, 2018
55,010	Publications distributed
64	News releases and announcements

* includes one representative complaint for each series of related complaints, see Appendix 2 - Statistical tables for more details

The *Personal Information Protection and Electronic Documents Act*

A year in review

CONSENT AND CONTROL

The centrepiece of last year's Annual Report to Parliament was our Report on Consent. In it, we carefully considered the obligation under PIPEDA that organizations obtain meaningful consent for the collection, use and disclosure of personal information.

In the era of data analytics, AI, robotics, genetic profiling and the Internet of Things, we recognized that the cornerstone of Canada's federal private sector privacy law was under considerable strain. Nevertheless, we concluded consent remains central to personal autonomy and should continue to play a prominent role in privacy protection, where it can be meaningfully given with sufficient information.

But consent, we said, must be supported by other mechanisms if we are to effectively protect privacy, including independent regulators that inform citizens, guide industry, hold it accountable, and sanction inappropriate conduct.

To that end, a number of our activities this past year were aimed squarely at bolstering consent and control under PIPEDA.

Consent guidance

Shortly after the 2016-17 Annual Report was tabled, we published draft guidance on consent and inappropriate practices which topped a list of 30 topics in last year's Report on Consent and on which we said we would begin issuing new or updated information and guidance, to the extent our limited resources allow.

We encouraged stakeholders to provide feedback and received 13 submissions, largely from associations representing businesses.

After reviewing the submissions, we revised the guidance and published final versions in May 2018. Our guidance on inappropriate data practices became applicable to businesses on July 1.

Our guidance on obtaining meaningful consent sets out practical and actionable advice for organizations. The guidance on no-go zones sets boundaries that protect individuals from the inappropriate data practices of companies.

Among other important advice in the meaningful consent guidance, including seven guiding principles, we outline four elements that must be emphasized in privacy notices and explained in a user-friendly way:

- what personal information is being collected;
- with which parties personal information is being shared;
- for what purposes personal information is collected, used or disclosed; and
- what risks of harm or other consequences might come from any collection, use or disclosure of the information provided.

For further details on the OPC's response to stakeholder feedback received on the draft guidance, including why certain changes were, or were not, made to the final versions, see:

Commentary of the Office of the Privacy Commissioner on feedback received through the 2017 consent guidance consultation

Some stakeholders have expressed concerns about our decision to include risk of harm among the elements. This decision flows from the definition of valid consent. It requires that an individual understand not only the nature and purpose, but also the potential ***consequences*** of the collection, use or disclosure to which they are consenting.

What we are referring to are those residual risks that might remain despite an organization's best efforts to apply mitigation measures designed to minimize risk and impact of potential harms. Only meaningful residual risks of significant harm must be included in notifications. By meaningful risk, we mean a risk that falls below the balance of probabilities but is more than a minimal or mere possibility.

Significant harm would be defined as in s.10.1(7) of PIPEDA and include:

- bodily harm,
- humiliation,
- damage to reputation or relationships,
- loss of employment, business or professional opportunities,
- financial loss, identity theft, negative effects on the credit record, and
- damage to or loss of property.

We also heard concerns about binding language in the original draft guidance. While it is clear we cannot use guidance to establish new legal standards, we do believe that our role as a regulator includes giving guidance that clarifies broadly framed PIPEDA principles and sets expectations as to how the law should generally be interpreted. Given that PIPEDA is so broad in its formulation, this type of guidance helps to provide individuals and organizations alike with a degree of certainty in how the legislation applies.

As such, in the final guidance, we distinguish between requirements and best practices or recommendations. It's an important and useful change that was recommended by stakeholders. In short, we have added a checklist that distinguishes between "must do's" (what we feel is a legal requirement) and "should do's" (what we feel is a best practice).

With respect to our new guidance on inappropriate practices, while context is of course important in the application of subsection 5(3) of PIPEDA, we firmly believe there is value in, and even a need for, specific

examples of practices that will generally be found inappropriate. This should set useful boundaries for individuals and organizations.

We will begin to apply our guidance on obtaining meaningful consent, which was issued jointly with our Alberta and British Columbia counterparts in January 2019. This will give organizations time to implement any necessary changes to their systems and practices. The OPC guidance on inappropriate practices became applicable as of July 1, 2018.

Reputation

The OPC identified reputation and privacy as one of four strategic privacy priorities in 2015. With the proliferation of social media and new communications technologies, we were concerned about the ease with which people can post information about themselves and others, and the difficulty of removing or amending information once it's online.

For example, an adult may feel their reputation is harmed by controversial views they held as a teenager and posted online. Other examples could include defamatory content in a blog; photos of a minor that later cause reputational harm; intimate photos; or online information about someone's religion, mental health or other highly sensitive information.

Our stated goal in identifying this as a priority was to work towards creating an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.

We launched a consultation and call for essays on the issue of online reputation. Based on the submissions received, along with our own analysis, we published a Draft Position on Online Reputation in January that champions solutions that offer a balance among freedom of expression, the privacy interests of individuals and the public interest.

The draft report concludes that Canadians have an existing right under PIPEDA to ask search engines to de-index web pages, and to ask websites to remove or amend content that contains inaccurate, incomplete or outdated information. The proposal draws parallels with the "right to be forgotten" in the European Union.

We also called for:

- greater protections for children and youth upon reaching the age of majority;
- privacy protection to be incorporated into curriculum for digital education across the country to help develop responsible, informed online citizens; and
- Parliament to study the overall issue.

While we recognize de-indexing is not necessarily a perfect solution to protecting reputation, it is nonetheless an important tool that we feel is available under the current law. Still, given competing rights on this issue, we believe it merits an examination by elected officials.

In fact, in its report on PIPEDA reform, ETHI carefully considered the issue, concluding the government ought to amend PIPEDA to include a framework for a right to de-indexing and web content removal based on the European Union model. At a minimum, the committee agreed stronger de-indexing and take-down protections for youth are needed.

In the meantime, our Office has continued to receive complaints relating to Google search results. In responding to one of these complaints, Google asserted that PIPEDA does not apply to its search engine service, contrary to the OPC's draft position, and that if PIPEDA did require de-indexing of lawful, public content, that would be unconstitutional.

In order to seek clarity on the threshold issue of whether PIPEDA applies to Google's search engine,

we plan to initiate a reference with the Federal Court. The reference will seek a determination as to whether Google's search engine service collects, uses or discloses personal information in the course of commercial activities and is therefore subject to PIPEDA, and whether Google is exempt from it because its purposes are exclusively journalistic or literary. Our position will remain in draft form and the complaints received will be kept in abeyance pending a resolution by the Court as to the applicability of PIPEDA.

Also in the context of online reputation, the 2017 Supreme Court of Canada decision in Google Inc. v. Equustek Solutions Inc. is worth noting. In this case, the court ruled that it was possible for a Canadian court to grant a worldwide interlocutory injunction against a search engine in order to have it delist websites. While the case had to do with trade litigation, it has implications for privacy and may have ramification for the "right to be forgotten" debate. For more information about this case, see the Privacy cases in the courts section of this report.

PIPEDA review

ETHI completed its study of PIPEDA in February 2018 with the release of a report entitled *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*. This included consideration of our Report on Consent, originally published in our *2016-17 Annual Report to Parliament*.

The OPC had a number of opportunities to make representations on PIPEDA reform leading up to the report's release.

We called for the OPC to have the authority to issue orders and the ability to impose administrative monetary penalties in order to deal effectively with those who would not otherwise comply with the law. In our submissions, we stressed that penalties would be imposed to promote compliance, not to punish, and would serve as an important incentive for organizations – noting that these powers would bring us in line with many of our international counterparts.

We also asked for new powers to conduct compliance reviews, even if a violation of PIPEDA is not immediately suspected. This would allow us to more proactively address privacy issues that are unlikely to become subject to complaint as they involve complex business models or opaque data flows of which few Canadians may be aware.

On that note, we argued for more flexibility in choosing which individual complaints to investigate in order to better utilize our limited resources. In addition, should we decline to pursue an investigation, we asked that individuals be granted some form of judicial redress, such as a private right of action.

We were pleased to see the committee conclude that there is a demonstrated need to grant our Office additional enforcement powers and that they took our concerns related to consent and reputation seriously. In some cases, the committee went beyond our recommendations for reforms, effectively calling for changes that would more closely align PIPEDA with the European Union's GDPR, which came into force in May.

As an example, the committee called for "privacy by design" to be legislated as a central principle for organizations to follow and for the right to data portability. The concept of privacy by design, coined by Ontario's former privacy commissioner, calls for privacy to be built in at the design phase of any new product or service.

In our representations, we also stressed the importance of maintaining Canada's "adequacy status" with the European Union. Since 2001, data has been

allowed to flow freely from the European Union to Canada. With the GDPR – the new European data protection instrument now in force – decisions about the adequacy of a country's privacy laws, in terms of whether they afford European citizens protections equal to those of Europe, will be reviewed every four years.

The committee was receptive to these concerns and called on the government to take appropriate action to ensure that the seamless transfer of data between Canada and the European Union can continue.

Last spring's allegations concerning Facebook and consulting firm Cambridge Analytica thrust privacy issues into the international spotlight. The case, which allegedly involved the collection of personal data from millions of unsuspecting Facebook users for the purposes of swaying political opinion, is now under investigation by the OPC and other regulators.

Not only has it proven to be a wake-up call to many that the time for self-regulation is over, it has also drawn attention to the lack of oversight over the personal information handling practices of political parties. This important gap, in part, prompted the Canadian government to introduce Bill C-76. However, the proposed legislation falls way short of international standards and adds nothing of substance in terms of privacy protection. Far more needs to be done to govern the use of personal information by political parties if the privacy of Canadians is to be adequately protected.

In the wake of this incident, ETHI undertook a review of the privacy implications of platform monopolies and possible remedies to assure the privacy of citizens' data and the integrity of democratic and electoral processes across the globe. The OPC participated in this review, and in June, ETHI published an interim report entitled Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process. The committee called on the government to take measures to ensure privacy legislation applies to political activities and reiterated the need for greater enforcement powers for the OPC. It commented that "the urgency of the matter cannot be overstated".

At the same time, the government came back with its response to ETHI's February report on PIPEDA reform. We are encouraged to hear the government agrees Canada's privacy laws need to be changed, but we are disappointed changes will likely have to wait several years, after the digital and data consultations take place and a federal election is held in the fall of 2019.

We ask the government to act immediately on ETHI's recommendations aimed at bolstering the enforcement tools in our toolkit – an idea broadly supported by parliamentarians, Canadians and privacy stakeholders.

In addition to our contribution to the ETHI committee study of PIPEDA, our Office participated in other parliamentary reviews that, at their heart, speak to issues of consent and individual control over personal information.

In particular, this involved our advice to the House of Commons Standing Committee on Industry, Science and Technology regarding Canada's Anti-spam Legislation, as well as our advice to the Senate Standing Committee on Transport and Communications regarding connected and automated vehicles in our section on parliamentary appearances.

Summary of key investigations related to consent and control

Microsoft: Giving Windows 10 users a say in what information they provide

In 2016, our Office launched an investigation into a complaint about the default privacy settings offered by Microsoft's Windows 10 operating system. We wanted

to find out if, during the Windows 10 installation process, users had the opportunity to give fully informed consent to the collection and use of their personal information by Microsoft.

Microsoft was cooperative with our Office in making changes to address our recommendations flowing from our investigation. That being said, Microsoft is one of the world's largest and influential companies, and its Windows operating system is used by over a billion individuals worldwide. We were therefore surprised that Microsoft had not proactively identified and addressed prior to the launch of Windows 10, the many privacy concerns ultimately raised by our Office's investigation and other data protection agencies around the globe.

During the course of our investigation, Microsoft issued two updates to Windows 10. The most recent, known as the "Creator's" update, included five new or updated privacy settings: location, diagnostics, tailored experiences, relevant ads and speech recognition. All five of them were set to "on" or "full" by default during the installation of the update. For each of these settings, we had raised concerns about whether Microsoft was giving users the information they needed to make a meaningful decision on consent.

For the "location" setting, for example, we recommended that Microsoft make it clear that third party applications could still determine a user's location even when this feature was turned off, and put in place measures to mitigate this risk. We also recommended that Microsoft make the default setting for the collection of diagnostic information from users' computers "basic" and not "full". We also called on Microsoft to develop a formal, documented protocol for ensuring that sensitive diagnostic data collected from users will not be used to deliver "tailored experiences".

For "relevant ads" we recommended that Microsoft clarify that this setting does not involve user consent for Microsoft's own relevant advertising practices, including a statement directing users to the separate mechanism that would allow them to choose whether and what "relevant ads" they would receive. Further, for "speech recognition", we recommended that Microsoft allow users to opt in, rather than forcing them to opt out of this feature, and that Microsoft delete any data collected contrary to users' speech recognition choices.

In response, Microsoft committed to implement a number of changes to address our concerns, beginning with having no pre-selected options for privacy settings during the Windows 10 installation. We are very pleased that users will have the choice to opt in to their desired privacy setting, rather than having to opt out of settings suggested for them. This sets a positive example for other companies wishing to obtain online consent for privacy settings.

Microsoft also committed to:

- enhancing privacy communications;
- augmenting privacy procedures;
- correcting and remediating any data collected contrary to users' speech recognition choices; and
- implementing measures to mitigate the risks associated with third party apps determining a user's precise location when the "location" setting is turned off.

In our assessment of the Creator's Update, we worked closely with our counterparts in the Netherlands. Based on the findings and recommendations flowing from their investigation and those of others, Microsoft made a number of changes to the European version of the software.

Although the Canadian version of Windows 10 is somewhat different, Microsoft's changes in Europe

are relevant and complementary to the findings of our assessment of the operating system. For example, Microsoft has made all settings opt-in, in keeping with our recommendation that users should have to provide explicit consent to send anything more than basic diagnostic information about their computer to Microsoft.

Read the report of findings on the Microsoft investigation.

Facebook: Company agrees to stop using non-users' personal information found in users' address books

In June 2013, Facebook notified our Office of a data breach involving contact information uploaded by Facebook users through the site's Contact Importer tool. A few days later, we received a complaint from an individual alleging that the company collected and disclosed the personal information of Facebook users and non-users without consent.

By way of background, Facebook's Contact Importer, also known as "Friend Finder," allows users to upload and store their contacts as part of their Facebook accounts. Facebook uses this information to suggest contacts with which users may want to be friends. It also allows users to send emails inviting contacts who are not on Facebook to sign up for their own account.

In 2012, Facebook engineers developed a process that associates pieces of contact information uploaded by different Facebook users with the same individual. For example, two users may have the same person in their contacts with the same phone number, but with different email addresses. By combining the different bits of contact information uploaded by different users, Facebook can more accurately determine whether a contact being uploaded by a user already has an account, and avoid sending that user an email inviting them to join.

Around the same time in 2012, a different set of Facebook engineers added a new feature to Facebook's Download Your Information (DYI) tool, enabling users to download a copy of all their imported contacts. However, due to what Facebook called an inadvertent coding error, the DYI tool downloaded too much information.

For each of the user's contacts, it also downloaded all the information that may have been collected from other users' address books and matched to that contact. As a result, according to Facebook, additional contact information belonging to some six million users around the world was disclosed, including some 142,000 users in Canada.

In addition, approximately 14 million pieces of contact information (email addresses and telephone numbers) that could not be connected to any Facebook users were also disclosed as a result of the breach. According to Facebook, it did not receive any complaints about misuse of data, nor did it detect any unusual behavior on the DYI tool or Facebook site to suggest wrongdoing or any harm to affected individuals in connection with the coding error.

In collaboration with Ireland's Data Protection Commissioner, we launched a coordinated investigation focusing on a number of issues raised by the breach, including whether Facebook is obtaining meaningful consent from users and non-users for the use of personal information during the matching process.

We found no issue with the way Facebook allows users to upload their contacts to their Facebook account. We did find, however, that the process of matching across address books constitutes a use of the personal information of users and non-users for which Facebook must obtain meaningful consent. The various notices Facebook offers to users do not include a clear description of the matching process or how it works. In particular, these notices do not explain

how a user's various pieces of contact information, including those imported by other users, will be used in the process of matching across address books.

Facebook disagreed with this finding, submitting that its users are provided with multi-layered notices about the collection and use of personal information in connection with the invite and friend suggestion functions. Moreover, it submitted that users join the platform for the purpose of connecting with friends and with the understanding that helping people connect is the whole point of Facebook.

Informed consent requires an understanding of the purpose, nature and consequences of the collection, use and disclosure of personal information. In this case, Facebook's use of contact information is aimed at enhancing a core service of connecting people on its social network. After considering Facebook's submissions, we agreed that, in this specific instance, the company has not changed its purpose for using Facebook users' contact information; it is simply using the contact information in a different way than historically to serve that purpose. In the circumstances, a user would still generally expect that contact information will be used to make friend suggestions. As a result, our Office concluded the consent issue to be not well-founded.

At the same time, we were not satisfied that Facebook was being sufficiently open with respect to how it handles contact information, especially when explaining how uploaded contacts will be used to help "you and others" find friends. Facebook does not explain what it means by "others." In this instance, we found the language to be unclear and did not adequately explain the matching process – that is, that Facebook combines and matches the contact information for a particular user with information that has been uploaded by other users.

Facebook advised that, while it respectfully disagreed with our conclusions on this issue, it would revise the notice for the contact import tool and the matching process. Accordingly, our Office determined the concern related to openness to be well-founded and conditionally resolved.

Following the issuance of our findings in this investigation, Facebook provided us with amended notices explaining the address matching process in the Contact Importer tool's Learn More pages, in the Help Center, on the uploaded contact management page and in its data policy. Our Office is satisfied that these amended notices now adequately explain the address matching process used by Facebook for the purpose of connecting people on its social network.

There was also the matter of Facebook's use of personal information belonging to non-users that is uploaded by users when they import their contacts to their Facebook account and is used in the matching process by Facebook. The company argued that, when it sends an email inviting a non-user to join, it explains how their information will be used. Again, we found the notice does not really explain how the matching process works. As well, we noted that in sending out the email, Facebook has already used the non-user's personal information, and has done so without their consent.

Without any workable way to obtain consent from non-users, based on our recommendation, Facebook is no longer keeping the matched contact information of non-users. Facebook has advised that from now on, the process of matching across address books no longer contains associations for contact information that has not been associated with an existing Facebook user, meaning that it is no longer maintaining the matched contact information of non-users. As a result, we determined this issue to be well-founded and resolved.

As part of this investigation, we also worked with Facebook to ensure it was giving users access to all contact information that had been matched to them, as well as the ability to correct this information. Facebook developed a short-term solution to provide

users with access to all contact information that had been matched to them and the ability to correct this information. As a result, we determined this issue to be well-founded and resolved.

Facebook also committed to develop a longer-term solution to this issue as part of its efforts to comply with the GDPR. We will continue to engage with Facebook on its efforts in developing such a longer-term solution for users.

Read the report of findings on the Facebook investigation.

Profile Technology: Company's re-use of millions of Canadian Facebook user profiles violated privacy law

We received complaints from a number of people alleging that their personal information had been collected from old Facebook profiles and groups and used to create new profiles on another social networking site called The Profile Engine (www.profileengine.com) without their consent.

The complainants said they discovered their information was posted on The Profile Engine by chance, when conducting internet searches for their own names. In one case, a complainant told us the information on the Profile Engine was lifted from a Facebook profile she had when she was a teenager, pointing out that anyone searching her name – including potential employers – would assume she was a very immature person. Another complainant stated that allegations of assault, which had been originally posted and then removed from Facebook, continued to appear on the Profile Engine.

The respondent, Profile Technology Ltd., argued that, since it was based in New Zealand and had no presence in Canada, our Office did not have jurisdiction to investigate and/or issue a report in this matter. We did not accept those arguments. In our view, there were several factors indicating a real and substantial connection between Profile Technology's activities and Canada to support our Office's jurisdiction to investigate the complaints, among others, the company's own claim that the website had close to 4.5 million Canadian profiles.

In any case, Profile said that it was simply a search engine that allowed people to find information that was already publicly available on Facebook, so consent was not needed. We determined that, while Profile may have originally collected individuals' profile information from Facebook for the purposes of providing search function services to Facebook users, it later copied and used the information for the new purpose of establishing its own social networking website.

In our view, this exception to consent does not apply since the profile information at issue was not "publicly available" as defined in PIPEDA regulations. Among other things, we considered that, unlike a publication such as a magazine, book or newspaper, Facebook profiles are dynamic and individuals maintain control over their profile information. Over time, users may update and change information, make their profile inaccessible to the general public or even delete their profile altogether. In our view, treating a Facebook profile as a publication would be counter to the intention of the Act, undermining the control users otherwise maintain over their information at the source.

We noted that all of the profiles and group information at issue in the complaints had either been removed from or changed on Facebook. In other words, the information only persisted on the Internet because it appeared on Profile's website. The profiles collected and re-used by Profile represented a snapshot in time. The company simply copied profiles, posted them on its own site and left them as they were when they were copied.

We determined that Profile had not obtained the individuals' consent to use their personal information in this way. It was clear to us that a reasonable

person would not consider Profile's use of the information to be appropriate in the circumstances. We recommended that Profile Technology delete all profiles and groups associated with any Canadians, including those associated with the complainants.

Profile refused the above outright. The company's blatant disregard for privacy obligations, along with their recalcitrance throughout the investigation – often providing cursory responses or failing to respond to our information requests at all – ultimately contributed to a lengthy investigation process into this complex matter.

Before we issued our report of this investigation, the company removed all of the profiles from its website. Since the information could no longer be indexed by search engines, this mitigated a key element of the complaints. However, Profile uploaded much of the information to the Internet (initially on the Internet Archive). The information was uploaded in separate database files with some identifiers removed and/or encrypted, making it widely available in this format for download via peer-to-peer sharing, including on the dark web.

As a result, we have no way of knowing how the data that Profile uploaded to the Internet may be used and disseminated in the future, to the extent that anyone is able to download, recreate the files, and exploit the information for their own purposes. A website operator, for example, could post the information and then charge individuals a fee to take it down, or the information could potentially be used to damage individuals' reputations.

In an effort to mitigate these kinds of risks, we contacted the Office of the Privacy Commissioner of New Zealand (NZ-OPC) to share our findings and discuss our concerns. The NZ-OPC agreed to review our report and consider what options may be available under the New Zealand Privacy Act and/or whether other New Zealand laws may apply. Our Office will continue to collaborate with our New Zealand counterparts to the full extent allowable under PIPEDA to support any further action to address this issue.

We also contacted Facebook to determine if they could inform our understanding of the database files posted by Profile on the Internet. Facebook confirmed that it was aware of the situation and that it was pursuing various avenues regarding the profile engine information, including via the courts, in relation to a court-recognized settlement.

Read the report of findings on the Profile Technology investigation.

Public Executions: Debtor-shaming website shuts down

The Office received a number of complaints about publicexecutions.com, a website that, for a fee, allowed anyone trying to collect a court-ordered debt payment to post details of the judgment on the site. In addition to posting the name of the debtor and the amount owed on the site, creditors, and anyone else, could post non-verified comments, along with other personal information about the debtor, including the debtor's address, photographs, or the kind of car they drove. Individuals listed on the website could be searched by name, and, in fact, the complainants' listings on the site were among top search engine results.

The complainants alleged the website breached their privacy rights under PIPEDA by publishing their personal information without their consent to, in effect, "name and shame" them into paying the debts.

The owner of the website argued that, because there was no "vendor-consumer" relationship with debtors, the disclosure of their personal information was not related to a commercial activity, and thus PIPEDA did not apply. He also argued that the website was a form

of journalism, further exempting it from PIPEDA's consent requirement.

Disclosing an individual's personal information in exchange for a fee from a third party is clearly a commercial activity, so PIPEDA did apply. As well, we found nothing to support the claim that the site was a form of journalism. A recent Federal Court decision (A.T. v. Globe24h) noted that to be considered journalism, an activity should involve an "element of original production." There was nothing original about the information on the site; it simply posted content provided by others.

Our Office's findings took into account the determination of the Ontario Ministry of Government and Consumer Services that the website unlawfully operated as an unregistered "consumer reporting agency" under Ontario's *Consumer Reporting Act*. As such, its use and disclosure of information relating to debts owing by individuals was strictly regulated under this legislation.

In this case, the website was disclosing personal information to the world at large. Accordingly, our Office found that, contrary to what is required by subsection 5(3) of PIPEDA, a reasonable person would not consider it appropriate for an organization to broadly publicize this information for financial gain and for the purpose of coercing debtors into paying their debts, given the availability of legal mechanisms to enforce judgments.

The owner of the website rejected our recommendation to delete all information relating to debtors from the website and also have the information removed from search engine caches.

We determined the complaints to be well founded. In light of our inability to order the owner of the website to delete all information from the website, the complaints remained unresolved, and, we were required to use our authority under PIPEDA to initiate legal proceedings with the Federal Court of Canada to have our recommendations enforced.

It was only after these proceedings were initiated that the operator of the website advised our Office that he had taken down the website and had no plans to reinstate it. As a result, our Office withdrew its application with the Federal Court but will continue to monitor to ensure the website is not reinstated in some form.

Read the report of findings on the Public Executions investigation.

Courier company: A company ends "delivery to a neighbour" after consent complaint

In this case, the complainant alleged that the courier company disclosed her personal information without her consent when it delivered a package addressed to her at a neighbour's house. The package, which the complainant was not expecting, was from a financial institution and contained sensitive financial information.

The company explained that, when a package requires a signature from the addressee and the person is not home, it would either deliver the package to a neighbour or drop it off at a pickup point. It stated that it offers "delivery to a neighbour" because many customers would rather not have to travel to a pickup point to retrieve their package. The company further explained that it obtains consent for delivery to a neighbour through the person or institution that is sending the package.

The company's terms and conditions for shipping packages mention that, if a package requires a signature, and the addressee is not home, then the courier company could deliver that package to a neighbour of the intended recipient. However, it is not clear that the courier expects the shipper to obtain the addressee's consent to leave the package with a neighbour.

We contacted the complainant's financial institution, which advised that it understood that if the addressee was not available to sign for the package, the person would have to pick it up at a store. The financial institution said it didn't know it was common practice to have a neighbour sign for a package.

We concluded that the courier company did not have the complainant's consent to have a neighbour sign for and accept the package on her behalf. We also found that the company did not make it clear to shippers how and when a package might be left with a neighbour, nor that the shipper was expected to obtain the addressee's consent for this.

In response to our recommendation that it ensure valid consent in the future, the company stated that, as of July 2018, it would no longer offer "delivery to a neighbour." We determined the complaint to be well-founded and resolved, based on the company's commitment to end delivery to a neighbour. Given that multiple players in the parcel delivery sector use similar neighbour-delivery techniques we encourage all companies to review their practices to ensure compliance with PIPEDA.

Read the case summary on the courier company investigation.

PIPEDA INVESTIGATIONS IN GENERAL

Overview

During the 2017-18 fiscal year, we accepted 297 complaints for investigation, and closed 311 investigations.

- As in past years, the financial sector continued to be the subject of most of the complaints we received under PIPEDA. This year, investigations of complaints involving the financial sector accounted for nearly a quarter (24% or 74) of all PIPEDA investigations.
- Organizations in the telecommunications sector (13% or 40), Internet (10% or 32), and services (13% or 39) sectors also attracted significant numbers of complaints.
- Also continuing the trend observed in recent years, Canadians were most likely to complain about issues related to access to their personal information (29% or 86) and consent issues (24% or 70) over the past year. Combined, these accounted for over half of all complaints accepted in 2017-18.

PIPEDA INVESTIGATIONS 2017–18

297 complaints accepted

Financial sector complaints accounted for nearly a quarter of all complaints received

More than half of the 311 cases closed dealt with matters related to consent (24%) and access to personal information (29%)

To make the most of our investigative resources, we continue to emphasize the use of early resolution to close straightforward complaints quickly and effectively. This year, two-thirds (66%) of PIPEDA complaints were closed via early resolution.

However, despite these and other successful efforts to increase efficiency, we continued to struggle to keep up with the demand for formal investigations and our backlog of files older than one year continued to grow. At the end of 2017-18, a third of our active investigations (55) were older than 12 months.

A number of factors impact our ability to close investigations within the 12-month timeframe set out in PIPEDA. The ease and low cost with which personal information can be collected, used and shared has reshaped the privacy landscape. The use of big data, AI and other technologies to derive value from raw data continues to grow.

These technologies – barely imaginable when PIPEDA was introduced – can have real and significant impacts on Canadians' privacy. More and more investigations require extensive technological analyses to first assess the privacy issues and then develop meaningful recommendations. Our investigation into a consent complaint about Microsoft Windows 10 described earlier in this report is just one example.

Our investigations are further complicated by the need to understand and remain current with the increasingly complex and fluid business models made possible by technology and data monetization.

Because our current model does not permit us to be selective as to which complaints merit investigation within our limited resources, these new complex issues must be investigated along with all other complaints that cannot be resolved to complainants' satisfaction through early resolution. In addition, without the backdrop of powers to order changes or sanction organizations with penalties for non-compliance, organizations can be slow to respond to our investigative inquiries and equally slow to commit to taking corrective action.

Other PIPEDA investigations

As demonstrated by the investigations summarized previously, technology has created a host of challenges for consenting to the collection, control and use of our personal information. Technology has also created new challenges for safeguarding personal information from unauthorized disclosure. PIPEDA requires that organizations protect the personal information they hold with safeguards proportionate to the sensitivity of the information – the more sensitive the information, the higher the level of protection that should be in place.

In the digital world, security cannot be a one-time thing. Safeguards must be reviewed on an ongoing basis to ensure sensitive information is protected from new and emerging threats.

PIPEDA doesn't specify what safeguards must be used, so it is up to organizations to identify the appropriate physical, technological and/or organizational tools necessary to ensure adequate protection of personal information. However, as the following investigation summaries demonstrate, in the digital world, security cannot be a one-time thing. Safeguards must be reviewed on an ongoing basis to ensure sensitive information is protected from new and emerging threats.

WADA: Agency improves deficient security measures for protecting athletes' personal information following investigation of global breach

As noted in last year's Annual Report, in September 2016, our Office became aware of a breach of the Montreal-based World Anti-Doping Agency (WADA), which oversees the international anti-doping regime for amateur sports. Specifically, a group

publically known as "Fancy Bear" disclosed on its website and elsewhere, the names of certain athletes who had competed in the 2016 Rio Olympic Games, along with their personal information which had been ex-filtrated from the Anti-Doping Administration and Management System (ADAMS).

To provide proper context and possible motive for this breach, it is important to highlight the dramatic events which occurred in the lead-up to the 2016 Rio Olympic Games. In July 2016, WADA released the findings of an independent investigation which confirmed certain allegations of Russian State manipulation of the doping control process at the 2014 Sochi Winter Olympic Games.[1] Russian whistleblowers had alleged state involvement in a massive doping operation in Russia, something that Russia has vehemently denied. Subsequently, the 2016 Rio Olympic Games took place from August 5 until August 21, 2016 and 118 Russian athletes were banned from competing.

Based on our investigation, it appeared the attack began with a phishing campaign: emails that appeared to be from WADA's Chief Technology Officer were sent to WADA employees, which compromised three WADA email accounts. Subsequently, the attackers gained access to an ADAMS administrator account and began using it to access information over the course of the next several days.

There can be no argument that much of the personal information contained in ADAMS is highly sensitive. The information consists of personal health information in the form of medical conditions, medications and prescriptions, analyses of bodily specimens and even genetic information outlined in an athlete's biological passport. In addition, ADAMS also contains anti-doping rule violations and information about an athlete's whereabouts.

The potential harms associated with the breach of this information are substantial and multi-fold. Unauthorized access and disclosure of certain personal health information can cause stigmatization, discrimination and psychological harm to individuals. The release of adverse analytical findings which, for legitimate reasons, have not otherwise been made public can cause embarrassment and shame to athletes, greatly impacting their reputation, image and personal and professional livelihoods.

All this suggests that in designing its safeguards, WADA must take into account the value of the information it holds to those who may seek to acquire it through nefarious means, and the prospect that it will continue to be the target of sophisticated attacks. It is noted that certain public reports have linked the Fancy Bear group to state-involved hacking efforts.

At the time of the breach, WADA had in place certain technological, physical and organizational safeguards. That said, there clearly were significant failings and their safeguard environment fell well below the level expected of an organization responsible for holding such highly sensitive medical information, with the potential to inflict significant damage on the reputation and integrity of athletes and the Olympic movement as a whole. WADA's need for an adequately robust safeguard framework is further informed by its status as a potential "high-value" target, for attacks by sophisticated hackers, including those of a state-sponsored nature.

In our preliminary report, our Office recommended that WADA augment its security safeguards to an appropriate level to protect the security and confidentiality of the sensitive personal information under its control by:

- developing a comprehensive information security framework which incorporates written policies and procedures to ensure that possible risks have been addressed;

1 WADA Statement: Independent Investigation confirms Russian State manipulation of the doping control process

- implementing appropriate safeguards related to access controls;
- employing adequate encryption protocols for ADAMS data in their custody;
- ensuring that application security and intrusion detection is properly configured and that systems and logs are adequately and actively monitored.

In response to our preliminary report, WADA agreed to implement all of the recommendations and accordingly, we concluded that the matter is well-founded and conditionally resolved. As such, our Office will be closely monitoring the organization's implementation of our recommendations and, to this end, has entered into a compliance agreement with WADA.

VTech: Toy-maker's failure to patch well-known vulnerability leads to massive data breach

In early December 2015, VTech Holdings Limited, a Hong Kong-based manufacturer of web-enabled electronic learning toys for children, notified our Office of a global data breach. According to the company, the personal information of over 300,000 children in Canada alone may have been compromised, including their names, dates of birth, photographs, voice recordings and chat discussions. VTech stated that the personal information of some 237,000 Canadian adults – mostly parents of the children affected – could also have been compromised.

Shortly after this notification, a Canadian affected by the breach filed a complaint with our Office. The complainant alleged that VTech failed to adequately safeguard the personal information of its customers, allowing hackers to access customers' information, possibly including his own and his son's.

The investigation, which benefited from collaboration with our international counterparts, the U.S. Federal Trade Commission and the Hong Kong Privacy Commissioner for Personal Data, found that the hacker accessed one of VTech's networks using SQL injection. This is a well-known and commonly exploited security vulnerability.

The investigation also revealed that, among other shortcomings, VTech did not test for vulnerabilities on a regular basis and, as a result, had not taken any action to protect its networks from this easily preventable attack.

VTech did act quickly to minimize the impact of the breach, notifying its customers by email and other methods and advising them of steps they could take to reduce the risk to their personal information. The company also committed to implementing a variety of measures to upgrade the security of its networks and safeguard its customers' personal information.

Accordingly, we found this complaint to be well-founded and resolved.

We note that, while this breach caused considerable concern and worry for VTech customers, including hundreds of thousands of Canadians, it is possible that very little personal information was compromised. The hacker, who was arrested, claimed he intended only to expose vulnerabilities in VTech security and had shared only a small amount of information with a reporter to show how easily he could access VTech's networks. The information that was disclosed was returned to the company.

Read the report of findings on the VTech investigation.

Access and airlines

Our Office also had the opportunity to investigate the treatment of access requests by airlines in two separate cases related to the disclosure of personal information by the airlines to third parties.

Jet Airways: Commissioner does not have authority under PIPEDA to compel documents subject to solicitor-client privilege claim

Two complainants with physical disabilities were removed from a Jet Airways plane following a disagreement with a member of the flight crew over the handling of their service animals.

Seeking compensation for the missed flight, the complainants asked the airline to provide them with access to their personal information relating to their booking and the incident in question. When the airline did not respond within 30 days, the complainants sent a second request, asking when and if the airline would comply with its obligations under PIPEDA. The response from a lawyer for Jet Airways indicated little more than that the request had been received.

The complainants contacted our Office, alleging that the airline was refusing to provide them with access to their personal information. Meanwhile, the complainants' representative wrote to the airline warning that, if the request for compensation was not settled in 30 days, a complaint would be submitted to other regulatory agencies.

The airline told our investigation that it didn't respond to the initial request because the person responsible had been on sick leave. Organizations are required to respond to a request for access within 30 days, even if it is refusing to provide access. The airline rejected our recommendation to put in place a mechanism to ensure it can meet this requirement in the future.

In any case, the airline said it was refusing access because the documents in question were created as part of a "formal dispute resolution process," and thus exempt under the Act. We found no evidence that the airline has a formal dispute resolution process, so this exemption would not apply. The airline disagreed with this finding.

Jet Airways also said it was justified in refusing access because the complainants said they might take their complaint to a regulatory agency. The airline said that, since this could lead to litigation, the legislation allowed it to claim solicitor-client privilege over any documents that could potentially be involved in future litigation at some point.

The Office does not have the authority to force an organization to produce documents in order to judge whether a claim of solicitor-client privilege is reasonable, and the airline refused to do so voluntarily or to provide details about the nature of the documents at issue. Without seeing the documents or having further information about them, we have no way of knowing whether this exemption was applied properly and therefore unable to make a finding as to whether the respondent was entitled to withhold the complainants' personal information on the basis of the exemption related to solicitor-client privilege.

That said, our Office had serious concerns that Jet Airways' privilege claims were overly broad. The airline initially indicated that it was internal policy for the organization to treat every incident as if potential litigation could occur; therefore, all documents and information created as a result were protected by privilege.

In our view, a blanket policy applicable to all documents generated from onboard incidents would not meet the tests for solicitor-client privilege and litigation privilege. While the airline no longer maintains its position that all documents generated as a result of an onboard incident are subject to litigation privilege, it did submit that it was entitled to claim privilege once the "legal notice" was issued. In our view, such a position is also problematic as it means potentially claiming privilege for documents that were created prior to a "legal notice" being received and which were not created for the dominant purpose of litigation.

We therefore found Jet Airways contravened Principle 4.1.4 by failing to adopt policies and practices that give effect to PIPEDA's principles.

We continue to encourage the airline to review the documents it may be withholding and release any that are not properly covered by solicitor-client or litigation privilege.

Read the report of findings on the Jet Airways investigation.

Airline company: Collection without consent and denial of access permitted by PIPEDA

After finding an individual did not have the documentation needed to enter Canada, security officials advised the airline on which the man planned to fly that he should not be allowed to board the aircraft. After the airline denied his request for a refund, the complainant asked the airline for access to all of his personal information in its possession, including any information that may have been exchanged with third parties.

The airline delivered some documents to the individual but, believing there was more information to be had, the individual filed a complaint with our Office.

The airline said it collected the complainant's personal information from a government institution in order to assess his travel status, and disclosed information about the complainant to a government institution investigating possible non-compliance with the *Immigration and Refugee Protection Act*.

Under PIPEDA, personal information can be collected without the knowledge or consent of the individual if:

- doing so would compromise the availability or accuracy of the information; and
- provided the collection is related to investigating a contravention of the laws of Canada or a province.

Information collected under this exemption also means that an organization is not required to give an individual access to that information. Moreover, under PIPEDA, personal information can be disclosed without the knowledge or consent of the individual by a private sector organization to a government institution that was investigating and gathering intelligence for the purpose of enforcing a law. Similarly, information disclosed under this exemption means that if the government institution objects, an organization must refuse to respond to the access request.

Based on the evidence, we determined that the airline applied these exemptions to consent and access properly, and we concluded this complaint to be not well-founded.

Read the report of findings on the airline company investigation.

Breaches

Over the past few years, there have been numerous high-profile data breaches involving industry giants in Canada and abroad that have adversely impacted the personal information of Canadians.

Over the past year, we have concluded globally relevant breach investigations such as WADA, and launched investigations into some of the most significant private-sector cyber breaches Canadians have seen to date: the incidents involving Bell Canada, Nissan Canada Finance, Uber and the Equifax credit-reporting agency are just some examples. These investigations are ongoing and we will share more details once we have closed these cases.

Data breaches, especially as a result of cyber-attacks like those summarized above, can compromise personal information belonging to thousands, even millions of Canadians. These types of breaches are occurring with increasing frequency, and the number reported to our Office was up again in 2017-18. Indeed, the number of reported breaches has doubled since 2014, when the government announced plans to implement mandatory breach reporting for private sector organizations.

In 2017-18, 116 private sector breaches were reported to the Office, an increase of 22% over the year before. As in previous years, the majority of incidents related to theft and unauthorized access (67%), followed by accidental disclosure (29%).

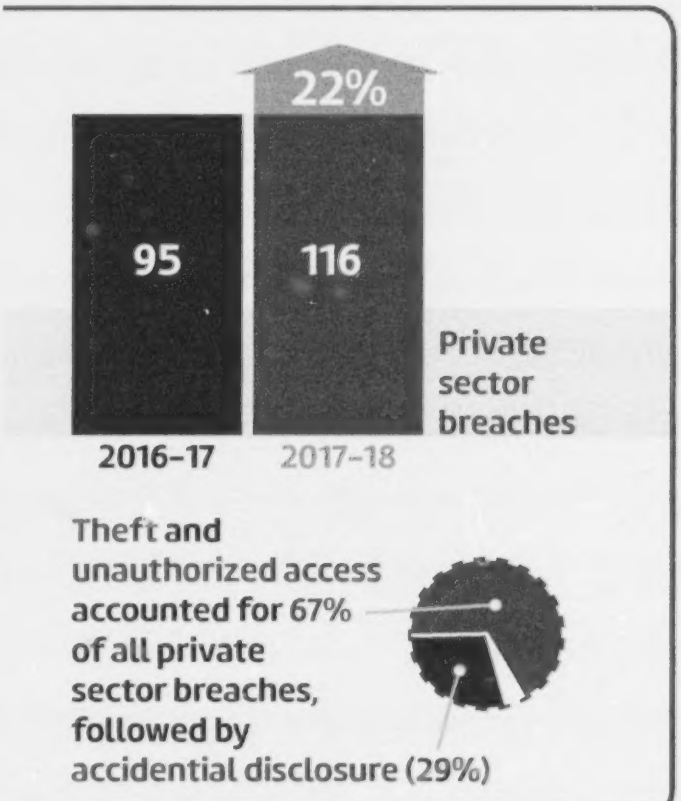
Of course these are the ones we know about. Given the sheer volume of personal data that is collected, used and disclosed in the digital marketplace, many cases likely go unreported, if not undetected. Breaches rightly breed fear among consumers and diminish confidence in the companies they do business with. Over time, this can lead to mistrust in the digital economy, which is in nobody's best interest.

Mandatory breach reporting for the private sector comes into force this fall without any associated funding for the OPC. With no funding for this activity and an already full plate, it will not be possible for us to devote the time necessary to properly review breaches and investigate. This is one of a number of resource pressures that have prompted us to request additional funding.

Starting in November, the law will require organizations to notify affected individuals, and to report to my Office all breaches they believe poses a real risk of significant harm to affected individuals, based on the sensitivity of the information involved and the probability it will be misused. Organizations must also maintain records of any data breach they become aware of and provide it to my Office upon request.

In April, Innovation, Science and Economic Development Canada published the regulations detailing how mandatory breach reporting and notification will work.

Publication of these regulations marks a long-awaited step in bringing data breach reporting into force. While mandatory notification is a move in the right direction towards enhancing privacy protection for Canadians, the regulations fall short.



We believe that breach reports to our Office should provide the Privacy Commissioner with information necessary to assess the quality of organizations' safeguards. Without this, our ability to improve security practices will be substantially hampered.

As well, such information would give us the opportunity to supplement information obtained through breach records, allowing us to develop a broad understanding of the overall challenges with respect to security safeguards and breaches in the marketplace. In turn, this would support our ability

to more effectively advise and guide organizations on how to improve their security practices and better protect Canadians' personal information.

We also believe that an effective breach reporting regime should include financial sanctions for not having adequate safeguards in the first place, not only for knowingly failing to report breaches after they have occurred. Sanctions for having inadequate safeguards would serve as an important incentive to prevent breaches, which should be the ultimate goal.

That being said, with our limited resources, we will be paying particular attention to how organizations address security vulnerabilities and assess the real risk of significant harm. We will also be monitoring how breach records are maintained by organizations, another new obligation under PIPEDA.

We are currently reviewing and updating our guidance regarding breach reporting to reflect the upcoming implementation of mandatory reporting.

PARLIAMENTARY ACTIVITIES RELATED TO PIPEDA

As described in greater detail earlier in this report, responding to emerging issues related to consent and control was a key focus of our Parliamentary activities related to PIPEDA during 2017-18. At the same time, as part of our mandate, we reviewed other legislative initiatives with the potential to impact on privacy, providing advice to Parliament as appropriate, making submissions, following up on an appearance or offering further views to Parliamentary committees studying these initiatives.

Among others, these activities included:

- participating in the statutory review of Canada's Anti-Spam Legislation (CASL);
- contributing to the Senate Committee on Banking, Trade, and Commerce study on cyber security and cyber fraud; and
- making submissions to the Senate Committee on Transport and Communications on the potential privacy impacts of connected, automated vehicles and on a proposal to require video and audio recorders in the cabs of railway locomotives.

Statutory review of Canada's Anti-spam Legislation (CASL)

As part of the statutory review of CASL, the House of Commons Standing Committee on Industry, Science and Technology invited our Office to provide its views on how the three-year old law is working and how it could be improved.

In his presentation, the Commissioner stated that CASL has been positive in helping to fight spam and address certain online threats, such as spyware, that can have a negative impact on Canadians' privacy. The Commissioner also noted that CASL provisions enabling us to collaborate and share information with the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau were key to the success of our investigation into address-harvesting and spamming by Compu-Finder.

At the same time, the Commissioner noted that this inter-agency information sharing allowed under CASL is limited to very specific circumstances. He recommended that either CASL or PIPEDA be amended to give our Office more flexibility to share information with the CRTC and the Competition

Bureau to address matters that intersect between consumer and privacy protection.

His recommendations also included proposing a change to indicate that CASL can add to the provisions of PIPEDA, but cannot lower its standards of protection. This would prevent a repeat of a situation in which an organization attempted to argue that it did not need to comply with PIPEDA because of an exception in CASL.

The Commissioner also recommended a change to PIPEDA to make it clear that, if someone installed spyware on a computer in violation of CASL, it would be a violation of PIPEDA to collect or use any information collected from that computer.

In its report, the Committee made a number of recommendations for changes to CASL, including giving the CRTC more flexibility to share information with enforcement partners. In the government response to the committee report, the Minister of Innovation, Science and Economic Development did indicate a readiness to consult with CASL enforcement agencies, including our Office, before introducing any amendments to the legislation.

Senate committee study on connected and automated vehicles

In January 2018, the Senate Standing Committee on Transport and Communications reported on its study into regulatory and technical issues related to the deployment of automated and connected vehicles.

Our Office participated in the study on two occasions: the Commissioner appeared before the Committee in March 2017, and the Office made a follow-up submission in November.

We were pleased that the Committee report reflected a number of our suggestions and concerns. The Committee issued several privacy-specific recommendations, including that the Government continue to assess the need for privacy regulations specific to connected cars, and that the OPC be empowered to proactively investigate and enforce industry compliance with PIPEDA in relation to connected vehicles.

Another recommendation called for Transport Canada to bring together relevant stakeholders such as governments, automakers, and consumers to develop a connected car framework, with privacy protection as one of its key drivers. The OPC would welcome the opportunity to participate in development of such a framework, should the government accept this recommendation.

Study and report on issues and concerns pertaining to cyber security and cyber fraud

In November 2017, the Commissioner appeared before the Senate Standing Committee on Banking, Trade and Commerce as part of its study on cyber-security and cyber-fraud issues.

Among other matters, the Commissioner referenced the mandatory data breach reporting regulations for the private sector that are to take effect in November 2018. The Commissioner stated that the regulations will be an important instrument for improving security practices of organizations, but could be improved.

As an example, the Office recommended that organizations reporting breaches should be required to include the information necessary to assess the quality of safeguards, and an assessment of the risk of harm. The Commissioner described this information as "critical" to establishing the baseline data needed to identify trends and address systemic issues, allowing for effective oversight.

Noting the significant disparity in the breach-reporting practices of government institutions, the

Commissioner reiterated previous recommendations regarding the modernization of the *Privacy Act*, including that breach reporting be made mandatory for federal institutions as well.

The Commissioner also spoke about the intersection of privacy and security, using proposed amendments to Bill C-59 as an example. The amendments call for the Communications Security Establishment (CSE) to have a role in sharing cyber-security information with other organizations. According to the proposed amendments, depending on the context, this information may include intercepted private communications.

While recognizing that the collection of all this data is necessary to effectively monitor networks, the Commissioner stated that it is equally important to ensure there are limits on the retention, use and sharing of personal information that is collected in this way.

The Commissioner concluded by emphasizing the importance of cyber-security specialists and data-protection authorities like the OPC working more closely together to improve the defences of our cyber infrastructure, and to ensure privacy protection is a guiding principle in cyber-security efforts.

Bill C-49, An Act to Amend the Canada Transportation Act and Other Acts

Bill C-49, a large omnibus bill addressing a variety of transportation-related matters, attracted our attention due to a provision to require railways to install locomotive voice and video recorders (LVVRs) in all trains.

During the Standing Senate Committee on Transportation and Communications study of the bill, we provided our views on a number of occasions: a written submission in September 2017; an appearance by the Commissioner in January 2018, and a follow-up submission in February 2018.

Our submissions focused on four areas of concern:

- the bill contained an unusual exemption from four key elements of PIPEDA: collection, use, disclosure, and retention;
- there was a lack of clarity on the continued role of the OPC in investigating alleged contraventions. The concern here was that the Office could have difficulty accessing LVVR recordings to determine whether they had been used in a way that breached an employee's privacy. We recommended that the bill confirm the jurisdiction of the OPC to investigate complaints relating to alleged violations of PIPEDA, including whether the exceptions to PIPEDA found in the *Railway Safety Act* were properly applied;
- we had concerns about whether individual rail employees would have a right of access to their personal information collected by LVVRs, as provided for by PIPEDA; and
- we recommended that the Committee clarify the scope of the regulation-making authority to guard against the possibility that regulations could be added that would expand the purposes for which collection, use, or disclosure of LVVR data is allowed.

In our February submission, we also noted that the OPC is rarely consulted during the legislative drafting phase of bills, and that Bill C-49 was no exception. We reiterated a previous recommendation that discussions with the OPC become a legal requirement under the *Privacy Act* when departments bring forth amendments that will have privacy implications. We believe our concerns could have been addressed earlier had we been consulted on the specific provisions of the bill.

Transport Canada ultimately committed to engage our Office during the regulation-making process to ensure that our concerns are addressed. We considered this commitment to be a constructive way forward.

We wrote to the Senate Committee to advise that we were satisfied with the department's efforts to address our concerns within the forthcoming regulations. Our letter also indicated that we maintained our position in principle on the issues we raised in our submission – most notably the exemption from PIPEDA requirements regarding the collection, use, disclosure and retention of personal information.

Finance Canada consultations

Our Office also provided submissions to Finance Canada. One concerned the privacy implications from changes to the retail payments oversight framework. As well, we provided views on positioning the federal financial sector framework for the future.

Our Office noted that while we support innovation, it is important to recognize existing privacy obligations for the sector. In addition, we outlined considerations with respect to emerging issues such as open banking and financial technologies (also known as fintechs).

In regard to fintechs, we raised concerns last spring about changes in the last budget implementation bill to broaden the types of organizations that may receive personal information from financial institutions.

While Finance Canada maintained the amendments would not reduce privacy protections, we disagreed. The amendments remove impediments for federally regulated financial institutions to share personal information with fin-techs, in our view, without ensuring parallel legislative measures are also adopted to address privacy.

We indicated that our preferred approach to addressing these concerns would be to strengthen PIPEDA to ensure that all organizations subject to the Act, not just financial institutions, obtain meaningful consent, and that the OPC be given adequate powers to ensure privacy rules are being followed, including the power to issue binding orders to organizations that fail to comply with the law.

The Commissioner noted the OPC had not been consulted on the amendments, which made it difficult to say whether the right balance had been achieved. With the information he had, he concluded while bill facilitates greater innovation, it does so without fully considering the impact on privacy. Despite our concerns, the bill passed unchanged.

CONTRIBUTIONS PROGRAM

Each year, the OPC's Contributions Program, launched in 2004 under PIPEDA, provides a total of up to $500,000 to support research conducted by academic and non-profit institutions, including industry associations, consumer and voluntary organizations, as well as trade associations and advocacy organizations. Applicants for funding are encouraged to propose projects that generate new ideas, approaches, and knowledge about privacy. These projects can help organizations better safeguard personal information, and help Canadians make more informed decisions about protecting their privacy.

Applicants for funding are encouraged to propose projects that generate new ideas, approaches, and knowledge about privacy. These projects can help organizations better safeguard personal information, and help Canadians make more informed decisions about protecting their privacy.

We issued two calls for proposals in 2017-18, generating a total of 49 proposals. Nine of these were selected for funding.

Among others, we supported two projects that studied the privacy implications of the growing number of "smart toys." Both projects found that these toys collect a significant amount of personal information using microphones, cameras and other sensors and, when connected to the Internet, often have security vulnerabilities that put a child's privacy at risk. The researchers found widespread use of data collection and analysis by toy makers, who provide very little information to consumers about what information is collected and how it is used or shared.

Another project the program funded was aimed at improving privacy for young adults with developmental disabilities. Based on their research, the project team developed a variety of learning tools to help young Canadians with developmental disabilities, as well as their families and the organizations that provide services to them, to identify and address potential risks to their privacy.

The *Privacy Act*

A year in review

NATIONAL SECURITY

When Bill C-51, the *Anti-Terrorism Act, 2015*, was tabled in the House of Commons in January 2015, we were among many Canadians who expressed concern that it failed to properly balance individual rights, including the right to privacy, with national security. Despite this, in August 2015, it was passed without amendment.

Since then, a commitment was made to repeal the problematic elements of Bill C-51 and introduce new legislation to strengthen accountability with respect to national security, and better balance collective security with rights and freedoms. The Commissioner, along with his provincial and territorial counterparts, made a formal submission as part of this process in December 2016.

Bill C-59

Following that consultation, Bill C-59, *An Act respecting national security matters*, was tabled in June 2017. In an appearance before the Standing Committee on Public Safety and National Security in December 2017, as well as in a written submission and a follow-up letter to the committee in March 2018, the Commissioner stated that while the bill was a step in the right direction, a number of concerns remained.

We proposed 11 amendments related to review and oversight, information sharing thresholds and the retention and destruction of personal information, among others. The government agreed with the vast majority of our recommendations and took measures to address many of our concerns. We of course welcome this development. The revised bill was passed in June by the House of Commons and is now awaiting consideration by the Senate in the fall.

In addition to the creation of a new National Security and Intelligence Committee of Parliamentarians (NSICOP) under Bill C-22, we were pleased with the proposal under Bill C-59 to create an expert review body (the National Security and Intelligence Review Agency, or NSIRA) with a broad mandate to examine the activities of all departments and agencies involved in national security.

Both of these bodies will be able to share confidential information and generally cooperate with each other to produce well-informed and comprehensive reviews that reflect considerations by experts and elected officials. Changes were also made to clarify the OPC's role in national security oversight. We too now enjoy the legal flexibility to share confidential information with NSIRA. Unfortunately, the same does not apply to interactions between the OPC and the NSICOP.

With respect to information sharing among federal institutions, Bill C-59 states that a government institution may disclose information when satisfied that the disclosure "will contribute to the exercise of the recipient's jurisdiction or the carrying out of the recipient's responsibilities... in respect of activities that undermine the security of Canada." There is also a requirement that "the disclosure will not affect any person's privacy interests more than is reasonably necessary in the circumstances."

This incorporates some aspects of the necessity threshold which we have repeatedly recommended. Another sign of progress was an amendment that requires recipient institutions to destroy or return personal information not necessary for them to carry out their mandate as soon as feasible.

Finally, we are satisfied with an amendment to the definition of "publicly available information" – namely, that it excludes information to which individuals have a reasonable expectation of privacy. We also called for an amendment to specify that publicly available information include that which is published or broadcast lawfully, and that information obtained through purchase or subscription is legally obtained or created by the vendor.

We're satisfied with a new principle added to the bill that addresses these concerns. The principle requires the CSE's activities, including those related to the collection of publicly available personal information, be carried out "in accordance with the rule of law."

We continue to track the progress of this bill, which is currently in the Senate, and remain hopeful that the final law will strike a much better balance between privacy and national security than existing provisions.

PRIVACY AT THE BORDER

On related issues, we also continued to raise concerns about privacy rights at the border, both in Canada and the U.S. President Donald Trump's executive order excluding non-citizens from the protections of the U.S. *Privacy Act* gave us an opportunity to highlight a serious gap in recourse available to Canadians travelling to the U.S., which we discussed in detail in last year's annual report.

Since that time, we have weighed in on Bill C-23, which authorizes American border officers to conduct preclearance activities, including searches on Canadians soil, and expressed serious reservations about the lack of standards to determine when it is appropriate to search someone's phone or other devices at the border.

Executive order

A number of Canadians contacted our Office in early 2017 to ask how an executive order issued by President Trump might impact their rights while travelling in the U.S. The order directed U.S. government agencies to ensure that their privacy policies exclude persons who are not U.S. citizens or permanent residents from the U.S. *Privacy Act* protections (to the extent consistent with applicable law).

The Commissioner wrote to the ministers of Justice, Public Safety and National Defence, both to seek clarity on travellers' protections and to urge them to determine whether U.S. authorities would uphold the

privacy protections included in various multilateral and bilateral agreements.

He also recommended the government request that the U.S. add Canada to a list of countries designated under the U.S. *Judicial Redress Act*. That law allows travellers from 26 European countries to apply for U.S. court review and remedy around certain privacy rights.

After exchanges with their U.S. counterparts, Public Safety Canada advised our Office that U.S. officials assured them that the executive order had not materially reduced privacy protections for Canadians.

We understand certain agreements would continue to be honoured and redress mechanisms would remain in place. Despite our recommendation and that of the House Standing Committee on Public Safety and National Security, the government declined to have the U.S. list Canada in the *Judicial Redress Act*.

Searches of electronic devices

In 2017-18, as we have in past years, the Office continued to review practices and receive complaints around how border officers (in both the U.S. and Canada) demand access to individuals' smart phones and other electronic devices. Parliamentarians were also engaged in the question, and in September 2017, during an appearance before ETHI, the Commissioner highlighted that Canada Border Service Agency (CBSA) officials continue to consider personal electronic devices to be simply "goods" in terms of their enforcement of the *Customs Act*.

As a practical consequence of that interpretation, any and all personal devices are subject to search at the border without any legal grounds. This is clearly an outdated notion and does not reflect the realities of modern technology. The Commissioner noted that while the policy of the CBSA is more nuanced, stating that electronic devices should not be searched without "evidence contraventions may be found on the digital device or media", he still recommended that CBSA policy should be elevated to a point of law through an amendment to the *Customs Act*.

Bill C-23 and preclearance areas at the border

In the context of Bill C-23, the *Preclearance Act, 2016*, electronic devices searches were also a focus for the Office, as expressed by the Commissioner on several occasions.

In addition to drawing attention to the issue in his appearance before the ETHI committee mentioned above, the Commissioner repeated these concerns in a letter and a follow-up letter to the House Committee on Public Safety and National Security, and in an appearance and subsequent letter to the Senate Standing Committee on National Security and Defence.

In these submissions, the Commissioner pointed to recent statements from the U.S. government noting their border officers could search the electronic devices of any non-citizen seeking to enter the U.S. at their discretion and without legal grounds. This would include requiring these individuals to provide the password to their cellphone and/or social media accounts.

The end result would be that a Canadian, even one still in Canada, could be ordered by a U.S. agent to hand over their smartphone and passwords at any time without cause, or be refused entry to the U.S.

In each of the Commissioner's appearances and submissions, he put forward, in several forms, the Office's recommendation that the preclearance legislation allowing such searches (Bill C-23) be amended to place border searches of electronic devices on the same footing as searches of persons; that is,

they could not be performed without "reasonable grounds to suspect."

While this recommendation was repeated by the House Standing Committee on Public Safety and National Security, the bill passed without significant amendment in December 2017 and subsequently received royal assent.

While we have been unable to convince legislators or the government to revise the law in this area, the government has committed to providing our Office with ongoing reports on the number of digital device searches being carried out by CBSA.

As well, we have a number of ongoing investigations related to national security and government surveillance, and are seeing heightened concerns from Canadians about privacy protections at the border and in the U.S.

We expect to report on border-related investigations in the near future. In the meantime, we have updated our guidance on privacy at airports and borders to ensure Canadians know what to expect when they travel. We note that Canadians may wish to exercise caution by limiting the number of devices they plan to bring to the U.S., and reviewing and limiting the information that is found on the devices they are taking with them.

PRIVACY ACT REFORM AND PARLIAMENTARY ACTIVITIES

For many years, our Office has been urging the government to modernize the *Privacy Act*, Canada's federal public sector privacy legislation.

We have made it clear that the Act is in desperate need of reform to bring it in step with technological change and to enhance transparency. Canadians agree it is time to modernize the Act, which has gone largely unchanged since it was introduced in 1983.

A survey commissioned by our Office and published in early 2017 found a majority of Canadians support amendments to the *Privacy Act*. The findings also indicated they want more accountability and transparency in their dealings with government.

While some legislators are listening, the government has been slow to act. We were very pleased when ETHI announced in March 2016 that it would undertake a study of the *Privacy Act*. Following the completion of its study, the Committee issued its final report, which concurred with virtually all of the recommendations our Office had put forward.

In April 2017, the government responded to that report, repeating a commitment made by the Justice Minister before ETHI in 2016 to lead a review aimed at modernizing the *Privacy Act*. The government said that this review "should give effect to Canadians' rights and expectations of privacy, promote public trust and facilitate good governance for our 21st century democracy."

We anxiously await the government's review and remain committed to working with them on modernizing this important law.

Parliamentary activities

In addition to the advice and other submissions to Parliament related to the issues of consent and control described earlier in this report, the Office continued, as a matter of routine, to monitor and comment on other legislative developments that could have an impact on Canadians' privacy.

Bill C-58: *An Act to amend the Access to Information Act and the Privacy Act*

While we awaited the government's review of the *Privacy Act*, the Commissioner appeared before Parliament to discuss the government's review of the *Access to Information Act* (ATIA), which has implications for the *Privacy Act*.

The ATIA and the *Privacy Act* have long been considered by the Supreme Court to be a "seamless code" of informational rights. The two acts work together to carefully balance both privacy and access. In previous comments on the ATIA, we had focused on the importance of maintaining this balance.

While we were pleased to see that Bill C-58 did not alter key concepts of public interest exception or the definition of personal information, it did introduce a provision giving the Information Commissioner the authority to order the release of government records, including records that may contain Canadians' personal information.

In an appearance before ETHI in October 2017, the Commissioner expressed concern that, in giving order-making power to the Information Commissioner, the bill would emphasize access to, over the protection of, personal information. In doing so, it would significantly and clearly disrupt the balance between access and privacy struck in the current legislation, and go against the Supreme Court of Canada's observation that privacy is "paramount" over access.

In his presentation to the committee, the Commissioner offered a number of recommendations for amendments to the bill, including that the Office be consulted in all cases where personal information is at real risk of being disclosed without the individual's consent.

The bill was referred to the Senate in December 2017 and was referred to the Standing Senate Committee on Legal and Constitutional Affairs for study in June 2018. We expect the Office will be invited to appear during the committee's study.

Statutory Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA)

In February 2018, the Commissioner appeared before the House of Commons Standing Committee on Finance as part of the statutory review of the PCMLTFA. The Commissioner reiterated concerns the Office has expressed in the past, pointing out that the Act, with a view to uncovering threats to national security or incidents of money laundering, casts a wide net that captures a great deal of information about law-abiding Canadians conducting financial transactions.

This information is collected by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Under the PCMLTFA, our Office has a mandate to conduct biennial reviews of the measures FINTRAC takes to protect the personal information it receives or collects. All of our audits have identified issues with FINTRAC receiving and retaining reports which do not meet legislative thresholds for reporting. We have recommended improvements, and FINTRAC has consistently responded that it will continue its work in implementing front-end screening measures to minimize the receipt of unnecessary personal information.

At the same time, we have generally found FINTRAC to have a comprehensive approach to security, including controls to safeguard personal information. Our most recent audit did identify governance issues between FINTRAC and Shared Services Canada (SSC), which holds FINTRAC data on its servers. FINTRAC has committed to addressing these issues.

The Commissioner presented several recommendations during his appearance before the Committee, including that the legislation be amended to allow the Office to offer advice on proportionality as part of our regular reviews of the PCMLTFA. In its most recent annual report, FINTRAC reported that it received almost 25 million records during the last fiscal year; however, in the same reporting year, there were only 2,015 disclosures to enforcement agencies for possible investigation.

We note that records that are not disclosed are retained by FINTRAC for 10 years. Even if one accepts that sharing financial transaction data related to law-abiding citizens may lead to the identification of threats of money laundering or terrorist financing activities, once that information is analyzed and leads to the conclusion that someone is not a threat, it should no longer be retained.

The Commissioner also recommended that, if changes to the legislation or the regulations are being considered, Finance Canada should be legally required to consult with our Office on draft legislation and regulations with privacy implications before they are tabled. The government recommended that the PCMLTFA be amended to provide that the reviews we currently undertake every two years occur every four years. We agreed with this recommendation. However, we recommended that the reviews take place at least one year before each five-year parliamentary review.

Our Office also echoed these views in our submission to Finance Canada's consultation on PCMLTFA.

PRIVACY ACT INVESTIGATIONS

Overview

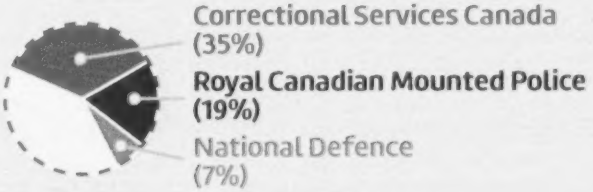
The Office accepted a total of 1,254 complaints under the *Privacy Act* during the 2017-18 fiscal year, down eight percent from the previous year. At the same time, we closed 1,208 complaints, an increase of 12% over 2016-17.

Complaints resolved through early resolution (ER) in 2017-18 took an average of more than four months, a 7% increase to the average over the year before. Complaints resolved through standard investigation took an average of almost 11 months, a month longer than had been the norm for the past few years.

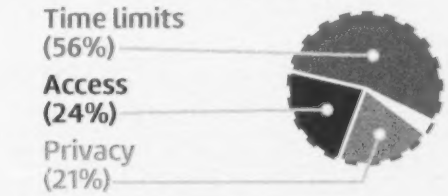
Despite continuing efforts to deal with complaints through our ER process – more than a third of *Privacy Act* complaints have been resolved through ER over the last three years – our average resolution time was a month longer this past year.

Complaints by the numbers

Top institutions by complaints accepted



Most common types of complaints related to



A number of factors played a role in increasing the average treatment time, including a deliberate decision to focus on resolving a number of older complaints that had been in the system for some time.

Meeting challenges to timely resolution

We strive to complete investigations and close complaint files within 12 months, but we are often working against circumstances outside our control.

The complexity of complaints received under the *Privacy Act* over the last five years, has grown significantly, as a result of the ever-increasing use of emerging technologies by federal institutions. As well, in many cases, federal institutions struggle to respond to inquiries from our Office in a complete and timely fashion, leading to lengthier and more resource-intensive investigations. We believe this is symptomatic of under-resourcing of access to information and privacy (ATIP) offices in some institutions.

We nonetheless have a responsibility to manage to the best of our capacity and continue to look for new ways to make the most of our limited investigative resources. Since 2010, we have undertaken a number of initiatives to address the issues that have the greatest impact on privacy, and these efforts continue.

In 2017-18, for example, we developed a revised online complaint form, which explains to complainants what our Office can and cannot do. We believe being up-front about our role and mandate will help us better serve Canadians. The new form, which we anticipate launching in 2018-19, is expected to improve the complaint receipt and registration process. We also introduced shortened final reports in instances where ER was not successful.

Using a risk-management framework, we have created a pool of unassigned, lower-risk files. This has reduced our investigators' workloads to a more manageable level and allowed a greater focus on investigations that carry a higher level of risk to Canadians' privacy.

We have also hired temporary resources to support our efforts to close some older files that present special challenges, including cases with difficult labour relations matters, or that involve institutions that are chronically slow and less forthcoming in their dealing with the Office. Together, these and other initiatives enabled the Office to reduce the number of complaints more than a year old by close to a third, bringing our total to 299 at the end of 2017-18.

Key investigations

As the examples summarized in this section show, the complaint investigations we concluded under the *Privacy Act* this past year covered a wide range of issues, from improper collection, use and disclosure of personal information, to questions of access to personal information held by federal institutions. These examples also provide some insight into how technology has added to the complexity of complaint investigations.

CSC once again erases video recordings while access request under review

The findings of this investigation were a source of significant concern to the Office, in that the federal institution involved has denied an individual access to his personal information in the same way it denied access to the same individual several years earlier.

By way of background, the complainant in this case – an inmate of a federal institution – submitted a series of complaints to our Office in 2011 alleging that Correctional Service Canada (CSC) had denied him access to his personal information. Specifically, he alleged that CSC was withholding video recordings he said would show correctional officers assaulting and harassing him. Our investigation found that CSC, contrary to the *Privacy Act*, had made no effort to retrieve the video recordings requested by the

complainant during their short retention period, simply allowing its video system to overwrite the recordings in question.

At the time, we recommended that CSC ensure that when requests are made for records that are normally kept for only a short time (such as video recordings, which are overwritten after 4.5 days) measures are in place to preserve and provide access to those records.

In 2016, the same individual contacted our Office to complain that CSC was again refusing to give him access to video recordings. CSC said it withheld some of the recordings for security reasons, as allowed under the Act. We reviewed those videos and agreed that this exemption had been applied properly.

However, for other recordings, we found that CSC had not taken steps to retrieve the videos requested by the complainant before they were overwritten, this, despite the fact that the complainant had submitted his request in time for them to be secured. We consider this to be a serious breach of the *Privacy Act* and determined the complaints of denial of access to be well-founded.

We were dismayed that, despite our previous findings that it had contravened the Act, and our recommendations to correct the problem, CSC had not taken any action to ensure its compliance with the Act. We have repeated that recommendation, which has been accepted by the CSC. In response, CSC stated that it will remind staff they must ensure videos are preserved and request for their access initiated immediately. It will report back to our Office within six months on what it has done to develop appropriate processes to ensure they are compliant with the legislation.

Read the report of findings on the investigation into a denial of access at the CSC.

IMSI-catcher at Warkworth Institution: CSC responsible for contractor intercepting text messages

We investigated several complaints alleging that CSC was using a cell-site simulator to capture and record cell phone conversations and text messages, without authority, at the Warkworth Institution located in Ontario.

The complaints followed an email the warden of the institution sent to staff, advising that he had authorized the use of a cell site simulator (or 'IMSI-catcher') to detect the use of cell phones by inmates, who are not allowed to have cell phones. In the email, the warden stated that the device collected information regarding cell phone location and use, as well as recorded all voice and text conversations, though the latter claim turned out to be inaccurate.

According to CSC, officials suspected that a series of safety and security incidents at the institution had involved the use of cell phones by inmates. To address this issue, CSC hired a contractor to use a cell site simulator to detect the presence and use of cell phones at the institution. CSC stated that, contrary to the warden's email, the contractor was authorized only to collect cell phone metadata, not to record conversations or texts. However, six text messages were captured by the device.

We confirmed that metadata from numerous cell phones used at the institution were collected. Metadata, since it may be revealing in terms of the identity and location of the cell phone user, it qualifies as the personal information of identifiable individuals as defined by the Act. Text messages also constitute personal information.

Under the Act, federal institutions can collect personal information only if the information relates directly to an operating program or activity of the institution. Given the risk to safety and security associated with unauthorized use of cell phones at the institution, it

Under the Act, federal institutions can collect personal information only if the information relates directly to an operating program or activity of the institution.

was our view the collection of cell phone metadata was consistent with the collection provisions of the Act in this instance.

As for the text messages, we found no evidence that CSC instructed the contractor to capture the content of cell phone communications. However, they were intercepted in the course of an activity carried out on behalf of CSC. Given its responsibility for the actions of the contractor, CSC thus contravened the collection provisions of the Act, and we determined this aspect of the complaint to be well-founded.

During the course of the investigation, CSC informed us that it does not intend to use cell site simulators in the future.

Read the report of findings on the investigation into the use of an IMSI catcher at the Warkworth Institution.

DND disclosure of medical records in sudden death investigations

Under paragraph 8(2)(e) of the *Privacy Act*, a government institution may disclose personal information without consent to an investigative body on written request for the enforcement of a law or for the purpose of carrying out a lawful investigation.

In this case, the complainants alleged that the Department of National Defence's Directorate of Access to Information and Privacy was, as a general practice, disclosing deceased Canadian Forces members' medical records to the Canadian Forces National Investigation Service (CFNIS) for sudden death (suicide) investigations without giving due consideration for the necessity of those records.

By way of example, the complainants' provided us with a copy of a request submitted by the CFNIS to the Directorate of Access to Information and Privacy at DND. In the request, the CFNIS asked for all records pertaining to the mental health and personal or family medical history of a Canadian Forces member.

The request stated that the information "will assist in determining [the deceased Canadian Forces member's] state of mind, and any condition or medications that may have affected his mental state, prior to his death."

In support of their position, the complainants referred us to the CFNIS Suicide and Attempted Suicide Investigation policy in place at the time, which stated:

> The investigation into suicide or attempted suicide should focus on determining that the wounds to the subject were in fact, self-inflicted…Administrative details (previous attempts, possible causes, marital status, alcohol or drug dependencies, etc.) need not be actively pursued…

The complainants' were concerned that the CFNIS appeared to be pursuing "administrative details" in its investigations and, by disclosing full medical records, DND was disclosing more than necessary to the CFNIS for its investigation purposes.

For its part, DND took the position that it was not required to determine whether the CFNIS was acting in accordance with its internal policies and that, in any event, an investigation completed by the Military Police Complaints Commission in 2015 found that CFNIS policies on suicide investigations were overly restrictive. As recommended by the Commission, the section of the policy saying that administrative details need not be pursued has been removed.

Our investigation looked at DND's policies and treatment of requests for medical information made by the CFNIS to DND's Directorate of Access to Information and Privacy under paragraph 8(2)(e) for the purpose of sudden death investigations, including suicides, over a period of several years.

We determined that this complaint was not well-founded. We noted that a disclosing organization has a responsibility for assessing whether the investigative body requesting the personal information meets the requirements of paragraph 8(2)(e), including a *prima facie* case that the requester is seeking only personal information directly related to its investigation. Based on the requests and related records we were able to review during the course of our investigation, we were satisfied that DND, as a matter of practice, had met its obligations in this regard.

We did note, however, that a Treasury Board Secretariat (TBS) directive requires that the section of the federal or provincial statute under which the investigative activity is being undertaken be stated in an 8(2)(e) request. Despite this requirement, for the requests from the CFNIS that we reviewed, requesters had simply put down either "*National Defence Act*" or "Sudden Death Investigation" as the authority for the requests.

Although we found that the disclosures were authorized under the Act, we also found that DND failed to retain copies of the "Request for Disclosure to Federal Investigative Bodies" forms in some instances. The Act, with its regulations, requires that institutions retain a copy of every request it receives for a minimum of two years, as well as a record of the information disclosed.

We recommended to DND that it update its policies and procedures to ensure that it confirms the authority under which the investigative body is conducting the investigation is referenced in requests made under paragraph 8(2)(e), and that all records relating to these types of disclosure requests are retained as required under the Act.

In response, DND agreed to implement our recommendations and will report back to our Office within six months.

Read the report of findings on the DND investigation.

Transport Canada orders drones to be labelled with personal information

We investigated four complaints against Transport Canada alleging that it was forcing owners of unmanned aircraft (UA) – often referred to as "drones," model aircraft or unmanned aerial vehicles (UAVs) – to disclose their personal information without consent.

At issue was an Interim Order issued by Transport Canada in June 2017, setting out a number of rules for so-called recreational users of UAs. The order stated in part, that "The owner of a model aircraft shall not operate or permit a person to operate the aircraft unless the name, address and telephone number of the owner is clearly made visible on the aircraft."

The order stated in part, that "The owner of a model aircraft shall not operate or permit a person to operate the aircraft unless the name, address and telephone number of the owner is clearly made visible on the aircraft."

The complainants pointed out that all other federally and provincially regulated forms of transport in Canada use registration numbers to identify vehicles, rather than requiring users to display personal contact information. They argued that displaying personal contact information on UAs could expose the operator to potential harassment or identity theft if the devices were lost.

Transport Canada says UA incident reports – which have increased by 200% since 2014 – support the notion that recreational users, who often have little experience as operators, are a risk to aviation safety, and to people and property on the ground. The department says it issued the Interim Order as a proactive measure to address the risk while formal regulations were being developed.

We note that an individual's name, address and telephone number are considered personal information and cannot be disclosed without consent. However, the disclosure provisions of the Act only apply to personal information under the control of a government institution. Here, since the order to label the UAs does not actually result in the collection of personal information by Transport Canada, the disclosure provisions of the Act do not apply. As a consequence, we determined the complaints to be not well-founded.

We recognize that all regulators are facing challenges related to UAs, including how to readily identify operators when problems arise. We note that unlike other vehicles, which require the operator to carry identification while in operation, UA operators are not physically with their aircraft. The Interim Order was issued pending the approval of revised regulations, which are expected to be published in the *Canada Gazette*, Part II, in 2018. Transport Canada assured our office that the revised regulations will take privacy concerns into account. While we did not have any recommendations to make in the context of this particular investigation, we do intend to monitor the development of the final regulations.

Read the report of findings on the Transport Canada investigation.

Statistics Canada: Legitimate concerns, but census data at no greater risk

We received a complaint against Statistics Canada (StatCan) alleging that the agency had improperly disclosed Canadians' confidential personal information (collected during the 2016 and earlier censuses), when it transferred management of its information technology (IT) infrastructure to SSC.

The complainant also alleged that, since the StatCan data is now stored in data centres shared with other federal institutions, there is a risk of unauthorized disclosure to those departments and agencies. The complainant was concerned that SSC employees with access to StatCan data were not supervised by StatCan, and questioned whether these employees had been sworn to confidentiality under the *Statistics Act*. He also questioned whether SSC would cooperate with StatCan audits of data security required to identify and address any potential security risks.

In the first instance, we found that StatCan did not disclose Canadians' personal information improperly.

Under the *Shared Services Canada Act*, StatCan is legally required to use the IT infrastructure services provided by SSC. Under this legislation, while information collected by government institutions may be stored on IT infrastructure owned by SSC, that agency does not own or control the information. This means, in this case, that StatCan still retains ownership and control of the data.

With regard to the concern that the data might be disclosed to other departments or agencies, we found that the StatCan data is stored in what had been a StatCan data centre before its ownership was transferred to SSC, and also housed in a segregated area of an SSC data centre.

As well, while ownership of the data centres was transferred to SSC, the census infrastructure is physically separate from IT infrastructure where other departments' data is stored – and technical and operational safeguards are in place to further reduce the risk of unauthorized disclosure. In addition, all SSC employees who have access to the census infrastructure – including employees that formerly belonged to StatCan – are officially deemed employees under the *Statistics Act*, and therefore subject to the same security provisions as StatCan employees.

As part of our investigation, we also reviewed the measures taken by StatCan to ensure that the personal census information of the tens-of-millions of Canadians transferred to SSC's IT infrastructure would be properly safeguarded. We looked at a number of documents provided by StatCan detailing

its arrangement with SSC, as well as the controls put in place to safeguard census data housed on SSC's IT infrastructure.

We note that our Office had previously made several recommendations to StatCan in response to the Privacy Impact Assessment (PIA) it submitted to our Office prior to the 2016 census. At the time, we recommended to StatCan that it should amend the PIA to indicate which technical systems were under the control of SSC, and include any assessments of privacy risks undertaken by SSC related to technical infrastructure under its control.

Based on this investigation, we were satisfied that StatCan had taken appropriate steps to safeguard the data held by SSC, and to mitigate the risks associated with the transfer of the management of its IT infrastructure to SSC.

In concluding our investigation, while the complainant raised legitimate concerns regarding the potential risks of transferring management of StatCan's informatics infrastructure to SSC, we determined this complaint to be not well-founded – since the personal information contained in the census records is still owned and controlled by StatCan, it was not in fact disclosed to SSC. In addition, we found no evidence to suggest a failure by either StatCan or SSC to adequately protect the data from unauthorized disclosure.

Read the report of findings on the StatCan investigation.

Canada Post: Mail forwarding system allows unauthorized disclosure

Canada Post Corporation (CPC) offers a mail-forwarding service that, for a fee, allows an individual to have their mail directed to another address for a period of up to one year. Individuals can arrange for the service at a postal outlet or through the CPC website. In either case, proof of identity is required. Among other methods, customers can verify their identity online through a link to a service operated by Equifax, a consumer credit reporting bureau. The customer is asked to answer a set of questions about their credit history and other unique personal information. If all questions are answered correctly, the customer's identity is verified and they can go ahead and arrange for their mail to be forwarded.

Mail forwarding only starts after three business days following the purchase of the service. According to the CPC, this three-day period served as a security measure. During this time period, CPC sends a 'Confirmation of Mail Forwarding' card to the old address before the service start date. Mail-forwarding cards ask receiving resident(s) to immediately contact CPC if they did not purchase the service.

In this case, someone impersonating the complainant used the online service to have the complainant's mail forwarded to another address. One day after CPC began forwarding his mail, the complainant received a Confirmation of Mail Forwarding service card in his name. He immediately contacted CPC, which stopped re-directing his mail.

According to CPC, the confirmation card was delayed due to a technical issue, and didn't get to the complainant until after it had started sending his mail somewhere else.

Our investigation found that the third party was able to impersonate the complainant by giving the right answers to all the questions on the Equifax verification system.

The Confirmation of Mail Forwarding Card uses an opt-out approach to ensure the validity of a service request. This means that an individual must take action if they do not want the service. We note that the process can fail if a card is lost, remains unread, or, as in the present case, is delayed. In our view, CPC

should devise and implement a more reliable control to address this issue.

We concluded that, because CPC failed to take all reasonable measures to ensure the information it used to forward the complainant's mail was accurate, the complaint was well-founded.

While we were investigating this complaint, CPC lengthened the period between the purchase of the mail-forwarding service and the start of the service from three to five days. While this might have prevented the unauthorized redirection of mail in this case, it still would not address situations where a card is delayed more than five days, is lost, or goes unread. We recommended that CPC devise a more reliable control that addresses the issues raised by our investigation. It agreed to do so. Therefore, we consider the matter to be conditionally resolved.

Read the report of findings on the CPC investigation.

Health Canada: Collection of detailed health information for drug benefits

An individual filed a complaint on behalf of some 20 physicians, claiming that Health Canada was forcing them to collect more personal information than necessary to process drug benefit claims from First Nations and Inuit people under the Non-Insured Health Benefits (NIHB) Program.

More specifically, the complaint dealt with the forms physicians must complete to claim benefits for one category of drugs on the Drug Benefit List, namely, "Limited Use Benefits." These are drugs that may or may not be covered by the program, depending on whether the patient meets the established criteria.

The physicians involved told us that, in many cases, Health Canada requests exact diagnostic information on the Limited Use Forms when, in their view, a general range would be enough to show that the patients met the criteria. A form for an arthritis drug, for example, requires the physician to state "the number of swollen joints."

The physicians said that, since the clinical criteria for the medication in question states that it is for the treatment of "severe active (Rheumatoid arthritis) with greater than or equal to 5 swollen joints," it should be enough to say that the patient is within the required range, rather than have to state the exact number of swollen joints. The physicians showed us forms for other drugs that also requested exact information rather than the ranges set out in clinical criteria.

Health Canada explained that the information requested on each form is based on clinical criteria defined by expert drug review committees. For the arthritis medication, the number of swollen joints is requested when the patient begins therapy with the drug, and again when the prescription is up for renewal, usually after a year. According to the criteria, if the patient's condition has not improved by more than 20 percent, for reasons of both patient safety and cost-effectiveness, the physician should choose a different therapy. Health Canada says a range in the number of swollen joints is not enough to make this calculation; it needs an exact number.

Based on the information provided by Health Canada, we concluded that the personal information collected on the Limited Use Drug claim forms is directly related to and necessary for the administration of the NIHB program, and therefore allowed under the *Privacy Act*. We determined this complaint to be not well-founded.

At the same time, the physicians told us that some patients have expressed concerns about how Health Canada stores, uses, and discloses their medical information, including information about their mental health. While these concerns were beyond the scope of our investigation, they show the importance that individuals place on maintaining control over their personal information.

We encouraged the department to engage with beneficiaries of the NIHB to explain the program's information handling practices – an issue we have raised with Health Canada in the past. By being more transparent, Health Canada can empower beneficiaries of the NIHB to exercise control over their personal information.

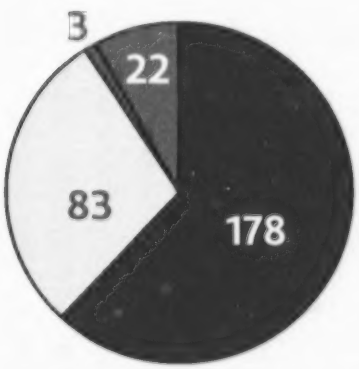
Read the report of findings on the Health Canada investigation.

Breaches

Federal institutions are required to notify both the OPC and TBS of all "material" privacy breaches – that is, a breach that involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or affects a large number of individuals.

It is up to federal institutions themselves to decide whether a particular data breach is a "material" breach, or whether a breach will be reported at all – there is no legal requirement to report beyond TBS policy. We have recommended the *Privacy Act* be amended to place a specific legal obligation on federal government institutions to report material privacy breaches to our Office. This would help us determine the extent of the problem across government, and allow us to provide advice and recommendations promptly to address the risks.

TYPES OF BREACHES REPORTED



In 2017-18, we received 286 public-sector breach reports. Although that is a significant increase over the 147 breaches reported in 2016-17, almost one quarter of those breaches are from a single institution whose reports were delayed by a year, highlighting the continuing downward trend in public-sector breach reporting.

We believe this is the tip of the iceberg. The response to an order paper question related to federal government privacy breaches tabled in Parliament gave us cause for concern. It revealed thousands of breaches affecting Canadians' information, including at least a half dozen large breaches concerning as many as 6,000 individuals, where institutions didn't notify those affected or our Office.

It prompted us to explore the issue of breach reporting under the *Privacy Act*. Our review, discussed in detail in the next section of this report, raised concerns about how seriously federal institutions take privacy.

Breach reporting review

As noted above, over the past number of years, the Office observed a steady increase in the number of public sector data breaches until 2016-17, when the number of reports dropped to less than half what it had been the year before. As we noted in last year's Annual Report, this caused us to wonder whether breach reporting requirements were being applied consistently across departments. We indicated then

that, in 2017-18, we would be following up with departments in order to understand the decline.

Review of privacy breaches in the federal government

Whether filing income taxes, applying for employment insurance benefits, or seeking a passport or a student loan, Canadians have little choice when it comes to entrusting their personal information to the federal government. Institutions are required to protect that information with appropriate measures, but our review of government breach reporting raises concerns about how they prevent and manage privacy breaches.

Why we undertook the review

Our Office uses the *Privacy Act* breach reports we receive from federal institutions to identify threats to privacy rights and to help determine where we should offer advice, recommend remedies or pursue enforcement. That's why we embarked on a review of government breach reporting to follow up on the puzzling decline in reporting in 2016-17, and other breach reporting issues we described in our previous Annual Report.

To be clear, the issues haven't changed since we tabled that report. We still receive reports from only a small number of federal institutions, and less than a handful of these involve cyber incidents.[2] We also continue to learn about what appear to be serious breaches through other channels, including the media, for example, a news report of paper files containing extensive personal details of hundreds of Canadians being lost as a result of a car theft.

How we carried out the review

We analyzed recent *Privacy Act* breach reports and reviewed related public sector statistics. We also engaged a dozen federal government institutions with large personal information holdings, and conducted an examination of their privacy breach procedures.[3] We did not invoke any of our formal powers in the conduct of this review, meaning that institutions' participation was voluntary. In that regard, we wish to acknowledge and thank these institutions for their time, efforts and frank comments.

We asked institutions if they would consider a lost valid passport to be a material (i.e., serious) privacy breach. They answered: "yes", "no", and "it depends".

What we learned

Based on government statistics, it is clear that thousands of breaches occur annually.[4] From our review, it is obvious that some material breaches go unreported and, more importantly, others likely go entirely unnoticed in many institutions.

On the latter point, many of the institutions in our review acknowledged that their employees, particularly front-line workers, don't fully grasp what constitutes personal information and their obligations under the Act. This is clearly a weak link in the chain to effectively prevent and manage privacy breaches.

Privacy accountability is also a problem. While breach reporting has been mandatory for four years, we found that the breach detection and review procedures of most of the institutions that took part in our review

2 Only two web hacking breaches were reported in FY 2017-18, which occurred on suppliers' systems, not the government infrastructure. This negligible number of cyber breaches is consistent with previous years, as outlined in our 2016-17 Annual Report to Parliament.

3 In-person meetings with senior ATIP, security and/or information technology officials from CBSA, CPC, CRA, DND, Employment and Social Development Canada, Global Affairs Canada, IRCC, Public Services and Procurement Canada, SSC and Statistics Canada; as well as written representations from CSC and the RCMP.

4 See responses to Parliamentary Written Questions Q-427 and Q-1465.

are missing key elements, and some don't have any approved breach procedures in place. Institutions do not have proper tools to assess the risk of injury or harm to individuals, focusing instead on assessing the risk to the institution.

Our review also confirmed that information technology safeguards for new systems aren't always what they should be, especially since these consistently involve the personal information of a large number of individuals. This was certainly evident in the findings of our Office's recent investigation into a series of incidents involving the Phoenix pay system, which determined that the breaches were the result of a combination of inadequate testing, coding errors, and insufficient monitors and controls of the system.[5]

Finally, we note institutions' frustration with a situation where direction and guidance around privacy breaches is inconsistently applied, sometimes ignored, and considered to be insufficient.

OPC observations and actions

We shared our insights with TBS, which is responsible for issuing direction and guidance to government institutions with respect to the administration of the *Privacy Act*, its regulations, and related policies. Specifically, we conveyed to TBS our findings that:

- The gaps in reporting, and the observations around privacy breach management in general point to a pressing need for better and clearer guidance, support, and training in respect of managing privacy breaches.
- Safeguards are likely to be ineffective unless and until institutions take meaningful steps to ensure that all employees understand what constitutes personal information. Privacy awareness for IT and security specialists should be considered on a priority basis in light of the government's admission that "cyber-attacks are becoming more pervasive, increasingly sophisticated and ever more effective,"[6] and given that most privacy breaches start out as security incidents.
- We have for many years advocated for the reform of the *Privacy Act*, calling for the inclusion of specific safeguard provisions and mandatory breach reporting. Our recommendations for legislative reforms have been supported by ETHI.

In its fourth report, ETHI recommends, in part, that the *Privacy Act* be amended to create an explicit requirement for institutions to safeguard personal information with appropriate physical, organizational, and technological measures commensurate with the level of sensitivity of the data.[7] In response, the government has launched a review toward modernizing the Act.[8] We look forward to a modernized law that protects the privacy rights of all Canadians.

TBS offered the following response:

The Government of Canada takes seriously its fundamental responsibility to protect the privacy of the personal information of Canadians. TBS is committed to ensuring that personal information is protected and secure, and looks forward to continuing to work with the Office of the Privacy Commissioner to strengthen the management of privacy breaches across the Government.

5 As outlined in the applicable report of findings, the institution subsequently accepted our recommendations to assist it in resolving the issues that contributed to the breaches.

6 Budget 2018: Equality + Growth – A Strong Middle Class, p. 203 (https://www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf)

7 Report 4 - Protecting the Privacy of Canadians: Review of the Privacy Act, section 2.3 (http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-4/page-51#s11)

8 Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics (http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-4/response-8512-421-135)

- TBS is developing an action plan for fall 2018 that will set out specific actions with specific timeframes to strengthen the management of privacy breaches across the Government.
- As part of this work, TBS will review its policies, tools and training for all employees and for privacy, security and IT specialists, to identify opportunities to strengthen guidance and tools for identifying, reporting and managing privacy breaches. For example, TBS will work with the Canada School of Public Service to review the "Access to Information and Privacy Fundamentals" course and the "Security Awareness Course," to strengthen their content regarding the protection of personal information and identification and reporting of privacy breaches.
- TBS will take action to raise government employee awareness of what constitutes personal information and their responsibility for privacy breach reporting, with priority given to IT and security specialists. For example, TBS will develop customizable privacy awareness tools, presentations, brochures and other products that can be used by Government of Canada institutions to raise employee awareness on privacy protection and privacy breaches, including in the context of Security Awareness Week.
- TBS will work with the Department of Justice to ensure that legislated data security standards and mandatory breach reporting are considered as part of the *Privacy Act* review.

Next steps

In the coming months, in collaboration with TBS, our Office will roll out a new *Privacy Act* Breach Reporting Form for Government of Canada institutions to facilitate reporting, assist institutions with the management of breaches, and bring greater clarity to the process.

Further, our Office will develop tips with respect to public-sector breach management, and promote them actively through both traditional, as well as newer and innovative, communications and outreach channels.

More importantly, however, we call on the government to leverage the findings of this study and address, on a priority basis, identified gaps to ensure the proper protection of Canadians' personal information.

ADVICE TO GOVERNMENT

The core responsibility of the OPC is to protect the privacy rights of Canadians. As discussed in the Commissioner's message, recent changes to our organizational structure have been adopted with a view to streamlining our work and enabling a more proactive and impactful approach to privacy protection.

This shift in our approach means putting greater emphasis on citizen empowerment. It also means working proactively with organizations – to the extent our limited resources allow – to better understand and mitigate any negative privacy impacts from any programs/activities, which would include technologies. By sharing information and advice during the design stage of new programs or activities,

we believe Canadians will be able to enjoy the benefits of innovation without undue risk to their privacy.

To bring additional focus to our proactive work with federal public sector institutions, our restructuring included establishing a Government Advisory Directorate. This group provides advice and recommendations in relation to specific programs and initiatives through a consultations function. It also reviews Privacy Impact Assessments (PIAs) and information sharing agreements submitted to the Office by federal departments and agencies. The directorate also undertakes outreach within the federal public sector in order to encourage compliance.

Consultations with government

The TBS *Policy on Privacy Protection* requires government institutions to notify the OPC Commissioner of any planned initiatives that relate to the *Privacy Act* or may otherwise impact on the privacy of Canadians – and to do so early in the planning process. This is to ensure the Commissioner has time to conduct a meaningful review of the proposed initiative, and to discuss any privacy issues identified with officials of the department involved.

In addition to consultations with the Office that are required under the policy, we also reach out to government institutions on a regular and less formal basis to offer advice, suggestions and recommendations on initiatives that could impact on the privacy rights of Canadians.

In 2017-18, government departments consulted us on a wide variety of initiatives that involved the collection, use and disclosure of Canadians' personal information, several examples of which are summarized here.

Transport Canada/World Economic Forum: known traveler digital ID

Transport Canada is working with the World Economic Forum and the private sector to develop a digital identity for travelers, which Canada is planning to test sometime in the next few years.

According to Transport Canada, the known traveler digital ID would give government agencies and private-sector organizations in different countries access to an individual's biometric, biographic and historical travel data, with the individual's permission.

This information would allow agencies to confirm an individual's identity and undertake a risk assessment in advance of the individual's arrival.

At the same time, digital IDs would ease international travel for individuals by allowing them to use their phones to access transportation and border control points through biometric recognition technology.

Developers of the technology believe it could be adapted for use in a number of sectors of the economy, including health care and banking. During our consultations, we offered some preliminary advice and recommendations on managing privacy risks – including the importance of safeguarding personal information related to the known traveler digital ID, limiting retention of information, and limiting secondary uses.

We were pleased to have been invited to offer our advice, given the extent, sensitivity and sharing of the personal information that would be involved, and we plan to consult with the department on an ongoing basis as the pilot moves forward.

CAF Sexual Assault Review Program and RCMP Philadelphia Model for Sexual Assault Review

The Royal Canadian Mounted Police (RCMP) and the Canadian Armed Forces (CAF) each consulted the Office about their plans to review historic sexual assault investigations. Both were considering adopting a form of the so-called Philadelphia Model.

This approach involves having an oversight body of external advocates and professionals, together with police representatives, review the case files of sexual assault complaints that had originally been ruled as unfounded.

Given the especially sensitive personal information that would be shared with third parties as part of the review process, we emphasized the critical need to fully assess the risks to privacy. We recommended to both the RCMP and CAF that they ensure that only the information necessary for purposes of the reviews be disclosed.

We also recommended the institutions consider how to inform the individuals involved in the original complaints about the potential disclosure of their personal information to an outside body.

Subsequent to our consultation, we received a PIA from CAF, in which they committed to posting a notice on the Canadian Forces website describing its Sexual Assault Review Program. While we offered some additional recommendations as part of our review of the PIA, we were pleased to note that it reflected many of the recommendations we made during our consultation, including measures to limit access to sensitive case files and a requirement for members of the review body to sign a non-disclosure agreement.

Meanwhile, the RCMP indicated its program remained at the exploratory stage and committed to work with our Office should it move forward.

National Inquiry into Missing and Murdered Indigenous Women and Girls: RCMP ends purge of old files

Following a document-preservation hold issued by the National Inquiry into Missing and Murdered Indigenous Women and Girls, the RCMP temporarily stopped purging files from a number of operational records management systems. The files in question had reached the end of their retention periods and would normally have been deleted, but were retained in order to preserve information that could be important to the Inquiry.

Given the risks of retaining information for extended periods of time, rather than stop purging old files altogether, we recommended that the RCMP review the files scheduled to be deleted and purge any information it could confirm was not subject to the preservation order.

We also recommended the RCMP restrict access to the information that was being retained for the purpose of complying with the order; ensure the information was not used for other purposes; and issue a public notice that the files in question were being retained for an extended period.

Following our consultation with the RCMP, it informed us that the inquiry had refined the scope of the hold. The RCMP accordingly resumed its purging of files as per stated retention periods.

Use of data analytics: CRA, IRCC and CBSA

We consulted with a number of federal institutions over the past year to discuss and advise on the use of data analytics and AI in delivering certain programs:

- the Immigration, Refugees and Citizenship Canada (IRCC) Temporary Resident Visa Predictive Analytics Pilot Project which uses predictive analytics and automated decision-making as part of the visa approval processes;
- the CBSA's use of advanced analytics in its National Targeting Program to evaluate the passenger data of all air travelers arriving in Canada, as well as its planned expanded use of analytics in risk assessing individuals;
- the Canada Revenue Agency's (CRA's) increasing use of advanced analytics to sort, categorize and match taxpayer information against perceived indicators of risk of fraud and non-compliance.

While we recognize the potential of advanced analytics to enhance government efficiency and support new ways to deliver services to Canadians, in our consultations with these institutions, we noted how these technologies may also encourage greater collection, sharing and linkage of data.

As a result, they also have the potential to be invasive, intrusive and discriminatory, depending on how they are used. We emphasized that these technologies should be adopted only after careful consideration of the privacy impacts. This would include an assessment of the necessity for using analytics in the first place, and whether the privacy risk involved in the use of analytics is proportionate to the outcomes being sought.

It is essential that the potential risks to privacy be considered now, when the application of analytics and artificial intelligence is still in its early stages within government. This means, among other things, considering ways to limit the collection of personal information to what is essential to effective operation of the technology; how to ensure the ongoing accuracy of the information held in these systems; and transparency, accountability and access – particularly with respect to information about how algorithms are impacting decisions being made about individuals.

Privy Council Office: Youth online consultations

The Privy Council Office launched an online process to encourage Canadians between the ages of 15 and 30 to share their thoughts on the themes and priorities they would like to see reflected in government policy. Youth could submit their opinions anonymously. In addition, they could participate in online forums or upload their own reports by registering on the website.

Participants could also upload videos to the consultation website through the third-party application GoodTalk. Before uploading videos, participants were asked to make sure they had consent from everyone appearing in their videos, including minors.

The Privy Council Office indicated that all videos submitted would be reviewed before being posted on the site, but it was not clear how it was going to confirm that everyone appearing in the videos had actually given their consent. We suggested that, in any future initiatives involving the posting of video content submitted by users, the Privy Council Office obtain written consent from all individuals appearing in videos. This is particularly important when minors are involved.

Statistics Canada: Increased use of administrative data sources

We have consulted with Statistics Canada (StatCan) on a number of occasions over the past several years to discuss the privacy implications of its collection of administrative data – such as individuals' mobile phone records, credit bureau reports, electricity bills, and so on. We spoke with the agency about this again in the past year, after a number of companies contacted us with concerns about StatCan requests for customer data.

StatCan says this kind of information is used to gain insight into various consumer trends, such as tourism and travel. It also helps in validating other necessary information such as household addresses and residential occupancy. The agency says that using administrative records that are already in existence is less expensive than other means of getting the information, while placing a minimal burden on respondents.

Although StatCan has informed us that it removes personal identifiers and uses the information only for statistical and research purposes, many Canadians might be surprised to learn the government is collecting their information in this way and for this purpose.

We have recommended the agency consider whether it could achieve the same objectives by collecting customer information that has been de-identified before it is disclosed to the agency. We also suggested it limit collection of administrative data to what is needed for the specified purposes, and that it evaluate the necessity and effectiveness of this work on an ongoing basis. To ensure transparency, we recommended StatCan let the Canadian public know how and why it is increasing its collection of data from administrative and other non-traditional sources.

Elections Canada: Register of Future Electors

Elections Canada and IRCC briefed our Office on the transfer of new citizenship data from IRCC to Elections Canada under Bill C-33: *An Act to amend the Canada Elections Act and to make consequential amendments to other Acts*.

In Bill C-33, the federal government proposes to create a Register of Future Electors. This would allow Canadians aged 14 to 17 to register voluntarily to have their information automatically added to the National Register of Electors when they turn 18. Young Canadians signing up for the register do not need consent from a parent or guardian to do so. However, for new Canadian citizens in the 14-17 age group, this option would be included on the Application for Canadian Citizenship for Minors. This form is filled out by the minor's parent or guardian. If the parent or guardian selects the appropriate box, IRCC will then provide Elections Canada with the young citizen's name, address, date of birth, gender, and unique client identifier.

This means new Canadians under the age of majority could have their names added to the register and their personal information disclosed from one federal institution to another without their knowledge. We recommended that IRCC consider the issue of meaningful consent in its assessment of the associated privacy risks.

Guidance on politically exposed persons and heads of international organizations

A politically exposed person or the head of an international organization is a person who holds a prominent position that comes with the opportunity to influence decisions and control resources – circumstances that can make them vulnerable to bribery or other forms of corruption.

Under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, financial institutions are required to determine whether a person is a foreign or domestic politically exposed person, the head of an international organization or a family member or close associate of such a person.

Enhanced due diligence measures, such as establishment of the source of funds for accounts and certain financial transactions, are required to be applied for all foreign politically exposed persons and for those domestic politically exposed persons and heads of international organizations who are determined to be a high risk for a money laundering or terrorist activity financing offence.

In June 2017, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) issued new guidance to financial institutions with regard to these types of account holders. We noted that the new guidance does not specify whether enhanced due diligence applies when a domestic politically exposed person or head of an international organization is assessed as a low-risk client. In our view, this creates a risk of over-collection of personal information from low-risk individuals.

We recommended and the Centre agreed to amend its guidance to specify that, except when required by regulation or legislation, enhanced due diligence measures do not apply to domestic low-risk politically exposed persons or heads of international organizations.

In response, FINTRAC committed to adjust its guidance to make this clarification and to publish frequently asked questions to enhance the transparency of obligations towards politically exposed persons and heads of international organizations obligations in this regard.

Privacy impact assessments (PIAs)

While the TBS *Policy on Privacy Protection* requires federal institutions to consult the Office early in the development of initiatives that may have implications for privacy, the *Directive on Privacy Impact Assessment* requires that institutions conduct a more thorough assessment of potential privacy risks in order to mitigate such risks prior to program implementation through the completion of a PIA.

Institutions are required to submit their PIAs to the Office for review, and we may recommend measures to further address risks to privacy. While our recommendations and advice are not binding, most institutions recognize the importance of a proactive approach to privacy, and work collaboratively with our Office to improve privacy protections.

CRA: information sharing with foreign tax authorities

For many years, the CRA and tax authorities in other countries have shared taxpayer information under a number of bilateral tax conventions and treaties. The Common Reporting Standard is a new international standard for the automatic exchange of financial account information between tax administrations to fight tax evasion.

Under the Standard, Canadian financial institutions report on accounts held by non-residents of Canada, as well as certain entities controlled by non-residents of Canada, to the CRA. The CRA will send this information, through formalized agreements, to the tax authorities in the countries where the affected individuals reside. The same applies to tax authorities in other countries, which will send information on accounts held by residents of Canada to the CRA.

In reviewing the PIA, we had some concerns about the potential over-collection and use of personal information by the CRA. As well, the PIA came to us before a number of Threat and Risk Assessments were completed. As a result, we had no way of knowing whether the risks involved in transferring data from the CRA to foreign tax administrations had been identified and addressed.

We were also concerned that the PIA didn't say what Canada has done or intends to do to satisfy itself that the receiving jurisdictions have appropriate safeguards in place to protect data provided under the agreements. We met with CRA officials to discuss these issues. At the time of writing, we were in the process of finalizing arrangements to review relevant documentation, including threat and risk assessment and security audit records, bilateral agreements and jurisdiction-specific confidentiality and data safeguard assessment reports.

CRA: Community Volunteer Income Tax Program

Every year, volunteers complete some 500,000 tax returns for low-income individuals at "tax clinics" hosted by community organizations or other groups. The CRA sponsors these clinics and registers the volunteers who complete the returns. While the vast majority of volunteers are interested only in giving back to their community, some breaches of the personal information collected have been reported to our Office in the past.

The CRA submitted a PIA on its Community Volunteer Income Tax Program to our Office, but it covered only the risks to personal information collected by the CRA when volunteers and community organizations registered for the program.

The PIA did not include an assessment of privacy risks associated with the handling of personal information by volunteers, including risks that the information could be used inappropriately or fraudulently. Among recommendations made by the Office to the CRA was that the scope of its assessment be expanded to include all aspects of the program.

CBSA: Primary Inspection Kiosks

In March 2017, the CBSA began the roll-out of its Primary Inspection Kiosks and a related mobile application called CanBorder-eDeclaration used in determining the admissibility of people and goods arriving in Canada by air. After landing in Canada, travellers are directed to a kiosk, where they scan their passport, have their photo taken, and answer a series of on-screen customs and immigration questions. With the app, travellers can use their mobile device to answer the basic declaration questions in advance, and the app sends a quick response (QR) code that can be scanned at a kiosk.

The kiosk runs the traveller's information through several CBSA databases, then prints a receipt that includes the traveller's photo and the results of the screening. The traveller hands the receipt to a CBSA officer, who checks it over and either releases the person to collect their baggage or refers them for additional questioning at secondary examination.

As part of our review of the PIA, OPC technical analysts conducted a technical review of the CanBorder-eDeclaration mobile app to assess the risk of web leakage. The review confirmed that data collected by the app is not transmitted and that locally-stored, temporary data is adequately protected.

In response to recommendations issued by our Office, the CBSA agreed to update the PIA to include additional information on how and when personal information may be disclosed to other government departments and law enforcement partners. On the other hand, it is our view that the agency has not justified retaining travellers' photos after they have completed their kiosk processing.

We also continue to encourage the CBSA to provide clear notice to travellers that the use of the kiosk is optional – if travellers prefer, they may bypass the kiosk (and avoid having their picture taken) by proceeding directly to a CBSA officer for screening.

Health Canada: Medical Cannabis Registration Program

Under the Medical Cannabis Registration Program, Canadians can register with Health Canada to grow and possess cannabis for medical purposes. Among other responsibilities, Health Canada receives and processes applications, verifies medical documents, and issues registration certificates.

In reviewing the PIA for the program, we recommended action to address a number of potential risks to privacy. In particular, we advised the department to enter into formal information sharing agreements with the various partners with whom it shares program information. We also encouraged the department to limit its collection of personal information to that which is necessary for administering the program. For example, we questioned the necessity of collecting non-drug related information from criminal record checks.

In addition, we requested details from Health Canada as to what measures were in place to address any risks associated with the possibility that individuals could be "re-identified" from anonymized registry data that is shared with municipalities. We also asked the department to explain to Canadians how the expected legalization of cannabis for recreational use will affect the program, and what happens to individuals' personal information when they decide to leave the program.

OPC report on historic PIAs: trans-border migration information sharing

As part of ongoing efforts to protect national and global security, Canada and its international partners share increasing amounts of information that is used to assess individuals arriving at their borders. Over the past several years, our Office has reviewed or been consulted on numerous PIAs relating to the sharing of information for immigration, asylum and travel determination purposes.

Given the number and variety of information sharing agreements that are now in place, we decided to review a sampling of these agreements and their related PIAs. Our goal was to identify any systemic issues or outstanding risks to privacy, and to better understand the evolution of this type of transborder information sharing.

We looked at a number of PIAs and consultations related to information sharing agreements initiated by IRCC, the CBSA, and Public Safety Canada between 2003 and 2016. We then assessed the agreements against a set of common criteria.

We expect information sharing agreements to be specific about what personal information is to be shared, and when and why it is being shared. We also expect these agreements to include provisions to limit secondary use and onward transfer of personal information, as well as a description of how the information is protected, how long it will be retained, and who is accountable for ensuring these provisions are respected.

In this regard, we note that the TBS *Guidance Document on Preparing Information Sharing Agreements Involving Personal Information* also sets out a number of provisions that are to be included in the agreements. We were disappointed to find that TBS provisions appeared only rarely in the agreements we reviewed and while attempts had been made to clarify information sharing practices, clauses generally fell short of our expectations.

All of the agreements we looked at explained why personal information was being shared, but many also talked about broader goals, which could allow for overly generous interpretations of circumstances in which information sharing is necessary.

As well, in setting out what information could be shared, many of the agreements we reviewed included wording such as "may include." This would seem to go against the spirit of our recommendation that institutions list exactly what personal information may be shared, and limit sharing to the information on the list.

Few of the information sharing agreements said anything about limiting secondary uses of the information shared. Those that did expressed them only in vague terms. We did find that most agreements contained at least some provisions for data security and retention, in keeping with our recommendation that information sharing agreements be specific about how personal information was handled. At the same time, we noted that agreements often operate in perpetuity – that is, there is no end date or any indication that the terms of or the need for information sharing be reviewed after a set period of time.

Perhaps most significant, our review found that, in general, consultations with the OPC had a positive impact on the development and drafting of ISAs. This was most evident in cases where the Office was engaged early in the process, or where the completion of a PIA coincided with – rather than followed – the drafting of an agreement.

In this context, we note our concern that not all trans-border information sharing activities at the CBSA and IRCC have been assessed by a PIA. While there is no formal policy requirement to conduct a PIA

in relation to information sharing activities, these activities do involve the use of personal information for administrative purposes and therefore demand some level of privacy assessment.

We hope to engage further with institutions related to their trans-border information sharing agreements to ensure such arrangements are subject to strong privacy protections.

Engagement sessions

Along with consulting on specific initiatives and activities and our work on PIAs, the Office also reaches out to departmental program and privacy officials on a proactive basis to offer general guidance on risk analysis and the conduct of internal reviews of personal information handling practices.

During 2017-18, this type of proactive engagement included a series of stakeholder engagement sessions with privacy and program staff across a range of federal departments and agencies. Along with numerous suggestions for possible improvement, we were encouraged by the many times participants emphasized the value they place on the advice and counsel provided by the Office – and that they would welcome earlier, more frequent and more informal consultations with us to better inform their privacy risk analyses. We are committed to be as proactive as possible in providing departments and agencies with advice that is both useful and timely.

Privacy cases in the courts

The Office continues to follow and, when appropriate, seeks to intervene in court actions that can impact Canadians' privacy rights.

CASES IN WHICH THE OFFICE WAS A PARTICIPANT THIS PAST YEAR

Attorney General of Canada v. Larry Philip Fontaine et al, 2017 SCC 47

In October 2017, the Supreme Court of Canada, upholding an Ontario Court of Appeal decision, ruled that survivors of residential schools should have control over the disposition of key records generated through the Independent Assessment Process (IAP) under the Indian Residential Schools Settlement Agreement (IRSSA).

The Government of Canada argued that the IAP records, which include personal stories of abuse told by thousands of survivors, are government files and subject to the provisions of the *Privacy Act*, the *Access to Information Act* and the *Library and Archives Canada Act*.

In the Supreme Court, as in the Ontario Court of Appeal, our Office again acted as an intervener, emphasizing the importance of ensuring residential school survivors had control over this highly personal information.

The Supreme Court affirmed that, under the terms of the IRSSA, it is up to residential school survivors to decide whether their stories will be archived or destroyed after 15 years.

Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN) v PGC-A-463-16 (Federal Court of Appeal) (decision pending)

We are currently awaiting a hearing before the Federal Court of Appeal on whether a Federal Court of Canada ruling on mandatory credit checks for correctional officers will be upheld.

As we reported last year, the Federal Court found that, since credit information can be useful in determining whether an officer may be vulnerable to corruption, it relates directly to the operation of TBS' security screening program and therefore it is allowed under section 4 of the *Privacy Act*. In addition, the Federal Court found that, contrary to the arguments made by the OPC, section 4 of the *Privacy Act* did not require that the collection of personal information be necessary for a government institution's operating program or activity.

As an intervener in both the original case and the appeal, OPC has taken the position that the relevant section of the Act should be interpreted to mean that government institutions must limit their collection of personal information to what is necessary to the operation of a program. In other words, institutions have to show that the personal information is not just "useful" to the operation of the program, but a necessity.

Her Majesty the Queen v. Ryan Jarvis, SCC 37833 (decision pending)

We are awaiting a decision in this case concerning a high school teacher who used a camera pen to record video of female students, often focusing on their chests. The teacher was first acquitted on a charge of voyeurism when the court found there was not enough evidence to show the videos were made for a "sexual purpose."

While finding that the recordings were made for a sexual purpose, the Ontario Court of Appeal upheld the acquittal, on the grounds that the recordings were made in circumstances where there was not a reasonable expectation of privacy – a key element in the voyeurism offence. A majority of the justices reasoned that, at school, students had to expect they would be observed and potentially recorded.

One justice offered a dissenting opinion, arguing that when at school, students do have a reasonable expectation of privacy with respect to anyone who would seek to compromise their personal and sexual integrity. This was the basis of an appeal to the Supreme Court of Canada, which the court heard in April 2018.

Our Office was among a number of interveners allowed to make a formal submission in the appeal. We argued that a "reasonable expectation of privacy" depends on more than location. Even in a public or semi-public setting, such as a school or office, individuals should be able to expect that certain aspects of their privacy will not be violated. In our opinion, the narrow, location-based approach taken by the majority in the Ontario Court of Appeal would undermine the privacy rights of Canadians in a range of situations.

CASES WE FOLLOWED WITH INTEREST

In addition to the cases in which the Office played an active part as intervener, there were a number of other cases touching on privacy issues before the courts, which we followed with interest.

Among others that attracted our attention were several cases heard by the Supreme Court of Canada:

- in *Douez v. Facebook* (2017 SCC 33), the court ruled on the enforceability of forum selection clauses in standard form consumer contracts when privacy rights are impacted – in this case, finding that a privacy related complaint against Facebook by an individual in British Columbia can be heard by a BC court, and does not have to be filed in California, as stated in the Facebook terms of use;
- in two separate cases, *R. v. Marakah* (2017 SCC 59) and *R. v. Jones* (2017 SCC 60), the court found that – depending on the circumstances – individuals can reasonably expect their text messages to remain private, even after they have been sent.

Although it did not have a direct impact on privacy, *Google Inc. v. Equustek Solutions Inc.* (2017 SCC 34) was of particular interest because it dealt with circumstances in which a search engine can be ordered to remove (de-index) information from its search results.

It also dealt with what is known as the "extra-territorial reach" of court orders; that is, whether a Canadian court can order a company without a physical presence in Canada to prevent harm that is occurring on the Internet. Both of these issues could have implications for the degree to which we can control our personal information on the Internet. Some of the privacy implications of the Equustek ruling on the issue of privacy and reputation are noted in the Consent and control section of this report.

International and domestic cooperation

The Office continues to engage with its counterpart organizations in Canada and other countries to better address cross-border privacy issues, and exchange knowledge and experience that can enhance privacy policies and standards around the globe. We also provide advice to the Government of Canada in assisting the government in developing privacy positions at international fora (such as the Organisation for Economic Co-operation and Development and Asia-Pacific Economic Cooperation).

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS

Commissioner Therrien was elected to serve a second two-year term on the Executive Committee of the International Conference of Data Protection and Privacy Commissioners at its 39th annual meeting in September 2017. The Executive Committee oversees the activities of the conference, the premier global forum for data protection and privacy authorities.

Building on enforcement collaboration work co-led by our Office last year, this year, participants adopted a resolution – which the OPC co-authored – on exploring future options for international enforcement cooperation.

In addition, participants adopted a resolution on data protection in automated and connected vehicles, which the OPC voted in favor of. The OPC also co-sponsored a resolution on enhancing collaboration between data protection authorities and consumer protection authorities. Flowing from this resolution, our Office is playing a key role in the *Digital Citizen and Consumer Working Group* and the drafting of its report to be tabled for the 40th annual meeting.

We are pleased to report that our Office, together with the Office of the Australian Information and Privacy Commissioner and the U.S. Federal Trade Commission, received both the Chair's Grand Award for Innovation, and the Award for Dispute Resolution, Compliance and Enforcement, at the inaugural International Conference of Data Protection and Privacy Commissioners Global Privacy and Data Protection Awards for the joint investigation of the Ashley Madison breach.

ASIA PACIFIC PRIVACY AUTHORITIES

In November 2017, with the Office of the Information and Privacy Commissioner for British Columbia, we co-hosted the 48th Asia Pacific Privacy Authorities (APPA) forum in Vancouver. Under the forum theme of Partnering for Research, discussions highlighted how partnerships with stakeholders from industry, civil society and academia can help inform and complement the regulatory and enforcement work done by data protection authorities and featured presentations on research funded under the OPC's Contributions Program.

GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN)

Working with the Ontario Information and Privacy Commissioner's Office, we "swept" 27 popular online applications used in classrooms from kindergarten through grade 12 as part of the 5th annual GPEN Privacy Sweep. The May 2017 Sweep focused on privacy practices of online educational tools and services targeted at classrooms. Many of the apps we looked at are taking important steps to protect the privacy of children and youth – but we also found cases where educational apps and websites were encouraging students to volunteer more personal information than necessary. Towards the sharing of enforcement strategies and skills, GPEN also held its inaugural Enforcement Practitioner's Workshop in Manchester UK. This leveraging of experience from various different global regulators was also co-led by our Office.

CANADIAN ANTI-SPAM LAW (CASL)

The Office was also among 10 agencies taking part in the first-ever Unsolicited Communications Enforcement Network (UCENet) Sweep led by the UK Information Commissioner's Office (ICO) and the Canadian Radio-television and Telecommunications Commission (CRTC).

The focus was on affiliate marketing, a commercial arrangement in which, for example, an online retailer will pay a commission to another website for referring consumers to its site, often by way of unsolicited texts or emails. The UCENet Sweep identified a number of issues, from misleading advertising to a lack of consumer consent. A number of websites were flagged for further action by the participating agencies.

The Office played a role in two reviews of CASL this year. An internal review with our domestic CASL enforcement partners generated largely positive findings, though it did lead to a call for greater information sharing and coordinated outreach activities among CASL partners.

The House of Commons Standing Committee on Industry, Science, and Technology, reporting on the mandatory three-year parliamentary review of CASL, also proposed giving the CRTC more flexibility to share information with its CASL enforcement partners. We note that we recommended such increased flexibility for sharing amongst partners, including the OPC, in the Commissioner's appearance before the Committee in October 2017.

FEDERAL–PROVINCIAL–TERRITORIAL COOPERATION

At the 2017 Annual Meeting of the Federal, Provincial and Territorial Information and Privacy Commissioners in Iqaluit, Nunavut in October 2017, we supported a joint resolution calling on governments to ensure that their Information and Privacy Commissioners (IPCs) have the authority to order public institutions to produce records they claim are exempt from access legislation, including claims of solicitor-client privilege. Without this authority, IPCs have no way to determine whether these kinds of claims are legitimate.

Another FPT collaboration involved youth privacy. Along with our partners we issued a joint letter to the Council of Ministers of Education calling for greater integration of privacy and digital literacy in schools.

We also worked with our provincial and territorial colleagues in the development of lesson plans for educators.

On the enforcement front, domestic offices with substantially similar legislation (Alberta, BC and ourselves) continued to identify opportunities for collaboration and information sharing through the Domestic Enforcement Collaboration Forum. Additionally, in April, 2018, we announced a joint investigation with the Office of the Information and Privacy Commissioner for British Columbia to determine whether Facebook and AggregateIQ are operating in compliance with PIPEDA and BC's privacy legislation.

SS7 PROACTIVE ENGAGEMENT

As part of increased efforts towards engaging in more proactive initiatives so that we might better understand complex technological processes and thus be in a position to advise organizations and better protect the privacy of Canadians, we made inquiries regarding SS7 (Signalling System No. 7). This is a set of signaling protocols which allow different telecommunications networks to speak with one another and share information related to connecting calls, roaming and billing.

Though known within the industry, a security vulnerability related to SS7 was brought to our attention last November in a report by the CBC and Radio-Canada that showed how hackers only needed a phone number to track the cellphone of an MP who had volunteered to take part in the exercise. This and other reports suggested hackers target SS7 to obtain subscriber information, eavesdrop on subscriber traffic, conduct financial theft, disseminate denial-of-service attacks and track location.

To gain a better understanding of the issue, the extent of its impact on privacy and what can or is being done to mitigate it in Canada and beyond, we reached out to government institutions already looking into the matter, as well as the Canadian Wireless Telecommunications Association, Canadian telecommunication companies, an international expert and our global partners.

We learned that SS7 is an essential tool for global communications. We understand that experts around the world, including Canadian telecommunications companies and government security agencies, are aware of this vulnerability and have been working together for some time to mitigate associated risks.

Some European countries, meanwhile, appear to be ahead of Canada in terms of mitigating the vulnerability.

Through our proactive engagement, we urged stakeholders to consider the following recommendations:

- take appropriate technical and organizational measures related to signaling security monitoring and filtering to manage risks posed to the security of networks and services;
- stay current on ongoing international best practices to secure interconnection for SS7, including GSMA (Global System for Mobile Communications Association) security best practices and guidelines, and implement these practices to ensure that an optimal level of protection is achieved; and
- make efforts to increase the awareness and knowledge of SS7 issues within their security and fraud teams.

We were encouraged by commitments from stakeholders in response to our recommendations and will continue to monitor the situation to ensure privacy issues remain top of mind when assessing and mitigating SS7 vulnerabilities. This issue once again illustrates the importance of continuously assessing existing and emerging technological threats to communications systems and networks.

Appendix 1 – Definitions

Complaint Types

Access:
The institution/organization is alleged to have denied one or more individuals access to their personal information as requested through a formal access request.

Accountability:
Under PIPEDA, an organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.

Accuracy:
The institution/organization is alleged to have failed to take all reasonable steps to ensure that personal information that is used is accurate, up-to-date and complete.

Challenging compliance:
Under PIPEDA, an organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.

Collection:
The institution/organization is alleged to have collected personal information that is not necessary, or has collected it by unfair or unlawful means.

Consent:
Under PIPEDA, an organization has collected, used or disclosed personal information without valid consent, or has made the provisions of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

Correction/notation (access):
The institution/organization is alleged to have failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

Correction/notation (time limit):
Under the *Privacy Act*, the institution is alleged to have failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

Extension notice:
Under the *Privacy Act*, the institution is alleged to have not provided an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or, applied a due date more than 60 days from date of receipt.

Fee:
The institution/organization is alleged to have inappropriately requested fees in an access to personal information request.

Identifying purposes:
Under PIPEDA, an organization has failed to identify the purposes for which personal information is collected at or before the time the information is collected.

Index:
Info Source (a federal government directory that describes each institution and the information banks – groups of files on the same subject – held by that particular institution) is alleged to not adequately describe the personal information holdings of an institution.

Language:
In a request under the *Privacy Act*, personal information is alleged to have not been provided in the official language of choice.

Openness:
Under PIPEDA, an organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Retention (and disposal):
The institution/organization is alleged to have failed to keep personal information in accordance with the relevant retention period: either destroyed too soon or kept too long.

Safeguards:
Under PIPEDA, an organization has failed to protect personal information with appropriate security safeguard.

Time limits:
Under the *Privacy Act*, the institution is alleged to have not responded within the statutory limits.

Use and disclosure:
The institution/organization is alleged to have used or disclosed personal information without the consent of the individual or outside permissible uses and disclosures allowed in legislation.

Dispositions

Well-founded:
The institution/organization contravened a provision(s) of the privacy legislation.

Well-founded, resolved:
The institution/organization contravened a provision of the privacy legislation but has since taken corrective measures to resolve the issue to the satisfaction of the OPC.

Well-founded and conditionally resolved:
The institution/organization contravened a provision of the privacy legislation. The institution/organization committed to implementing satisfactory corrective actions as agreed to by the OPC.

Not well-founded:
There was no or insufficient evidence to conclude the institution/organization contravened the privacy legislation.

Resolved:
Under the *Privacy Act*, the investigation revealed that the complaint is essentially a result of a miscommunication, misunderstanding, etc., between parties; and/or the institution agreed to take measures to rectify the problem to the satisfaction of the OPC.

Settled:
The OPC helped negotiate a solution that satisfied all parties during the course of the investigation, and did not issue a finding.

Discontinued:

Under the *Privacy Act:* The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for various reasons, but not at the OPC's behest. For example, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Under PIPEDA: The investigation was discontinued without issuing a finding. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

No jurisdiction:

It was determined that federal privacy legislation did not apply to the institution/organization, or to the complaint's subject matter. As a result, no report is issued.

Early resolution (ER):

Applied to situations in which the issue is resolved to the satisfaction of the complainant early in the investigation process and the Office did not issue a finding.

Declined to investigate:

Under PIPEDA, the Commissioner declined to commence an investigation in respect of a complaint because the Commissioner was of the view that:

- the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
- the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or,
- the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of PIPEDA.

Withdrawn:

Under PIPEDA, the complainant voluntarily withdrew the complaint or could no longer be practicably reached. The Commissioner does not issue a report.

Appendix 2 – Statistical tables

STATISTICAL TABLES RELATED TO PIPEDA

Table 1

PIPEDA complaints accepted* by industry sector

Industry sector	Number	Proportion of all complaints accepted **
Accommodations	19	6%
Entertainment	5	2%
Financial	70	24%
Food and beverage	2	1%
Government	2	1%
Health	4	1%
Individual	1	0%
Insurance	21	7%
Internet	31	10%
Manufacturing	4	1%
Not-for-profit organizations	1	0%
Professionals	18	6%
Publishers	3	1%
Sales/retail	16	5%
Services	43	14%
Telecommunications	40	13%
Transportation	17	6%
Total	**297**	**100%**

* PIPEDA complaints accepted based on count of one for each series of complaints dealing with related issue; excluded complaints total six

** Figures may not sum to total due to rounding

Table 2

PIPEDA complaints accepted* by complaint type

Complaint type	Number	Proportion of all complaints accepted**
Access	86	29%
Consent	70	24%
Use and disclosure	62	21%
Safeguards	45	15%
Collection	15	5%
Retention	5	2%
Accuracy	5	2%
Openness	3	1%
Accountability	2	1%
Correction/notation	2	1%
Appropriate purposes	1	0%
Other	1	0%
Total	**297**	**100%**

* PIPEDA complaints accepted based on count of one for each series of complaints dealing with related issue; excluded complaints total six

** Figures may not sum to total due to rounding

Table 3

PIPEDA investigations* closed by industry sector and disposition

Sector category	Early resolution (ER)	Dispositions (not ER)									Subtotal of dispositions not ER	Total early resolution and other dispositions
		Declined	Discontinued (under 12.2)	No jurisdiction	Withdrawn	Settled	Not well-founded	Well-founded	Well-founded resolved	Well-founded conditionally resolved		
Accommodations	12		1			1			1		3	15
Entertainment	3								1		1	4
Financial	48	2	13			2	4	1	3	1	26	74
Food and beverage	1											1
Government	1			2							2	3
Health	2		1						1		2	4
Individual				1							1	1
Insurance	15		2		2	1	2		1		8	23
Internet	14		7	3	3	1	1	2		1	18	32
Manufacturing	5								1		1	6
Not-for-profit organizations	1									1	1	2
Professionals	15		2		3		1	1	1		8	23
Publishers	1							1			1	2
Sales/retail	11					1			1		2	13
Services	33		1		1	1	1		2		6	39
Telecommunications	28		6						5	1	12	40
Transportation	15		4		1		3	2	1	2	13	28
Not specified									1		1	1
Total	**205**	**2**	**37**	**6**	**10**	**7**	**12**	**7**	**19**	**6**	**106**	**311**

* PIPEDA investigations based on count of one for each series of related complaints; excluded complaints total eight

Table 4

PIPEDA investigations* closed by complaint type and disposition

Complaint type	Early resolution	Discontinued (under 12.2)	Declined	No jurisdiction	Withdrawn	Settled	Not well-founded	Well-founded	Well-founded resolved	Well-founded conditionally resolved	Total
Access	63	9	1	1	2	1	4	3	10	1	**95**
Use and disclosure	43	12	1	1	2	1	2	2	4	1	**69**
Consent	38	8		4	5	2	1	2	3	2	**65**
Safeguards	29	4				2			2	1	**38**
Collection	8	2			1		3				**14**
Accuracy	11										**11**
Openness	4					1					**5**
Correction/notation	3	1					1				**5**
Retention	3										**3**
Accountability	2									1	**3**
Appropriate purposes	1	1					1				**3**
Total	**205**	**37**	**2**	**6**	**10**	**7**	**12**	**7**	**19**	**6**	**311**

* PIPEDA investigations based on count of one for each series of related complaints; excluded complaints total eight

Table 5

PIPEDA investigations* – Average treatment time by disposition

Disposition	Number	Average treatment time in months
ER-resolved	205	3.5
Discontinued (under 12.2)	37	8.3
Well-founded resolved	19	19.0
Not well-founded	12	18.0
Withdrawn	10	12.0
Well-founded	7	13.2
Settled	7	10.6
No jurisdiction	6	6.6
Well-founded conditionally resolved	6	19.6
Declined	2	2.0
Total cases	**311**	
Overall weighted average		**6.1**

* PIPEDA investigations based on count of one for each series of related complaints; excluded complaints total eight

Table 6

PIPEDA investigations* – Average treatment times by complaint and resolution types

	Early resolution (ER)		All other resolutions (not ER)		All investigations	
Complaint type	Number of cases	Average treatment time in months	Number of cases	Average treatment time in months	Number of cases	Average treatment time in months
Access	63	2.8	32	13.1	95	6.3
Use and disclosure	43	2.4	26	9.7	69	5.2
Consent	38	2.6	27	12.6	65	6.8
Safeguards	29	2.7	9	11.8	38	4.8
Collection	8	4.7	6	17.3	14	10.1
Accuracy	11	3.8			11	3.8
Openness	4	2.5	1	13.3	5	4.7
Correction/notation	3	2.2	2	7.7	5	4.4
Appropriate purposes	1	6.0	2	19.5	3	15.0
Accountability	2	1.4	1	39.0	3	13.9
Retention	3	0.9			3	0.9
Total	**205**	**2.7**	**106**	**12.6**	**311**	**6.1**

* PIPEDA investigations based on count of one for each series of related complaints; excluded complaints total eight

Table 7

PIPEDA voluntary breach notifications by industry sector and type of incident

Sector	Incident type				Total incidents per sector	% of total incidents*
	Accidental disclosure	Loss	Theft	Unauthorized access		
Accommodations	2		1	5	**8**	**7%**
Agriculture, forestry, fishing and hunting				1	**1**	**1%**
Entertainment			1	1	**2**	**2%**
Financial	12	2	3	10	**27**	**23%**
Government	1	1		1	**3**	**3%**
Health	1		2	1	**4**	**3%**
Insurance	5		1	1	**7**	**6%**
Internet				5	**5**	**4%**
Manufacturing				3	**3**	**3%**
Mining and oil and gas extraction	1		3		**4**	**3%**
Not-for-profit organizations	5		2	3	**10**	**9%**
Professionals				3	**3**	**3%**
Publishers				1	**1**	**1%**
Sales/retail	1			10	**11**	**9%**
Services	2		2	7	**11**	**9%**
Telecommunications	2		2	3	**7**	**6%**
Transportation	1			3	**4**	**3%**
Not specified	1	1	1	2	**5**	**4%**
Total	**34**	**4**	**18**	**60**	**116**	**100%**

* Figures may not sum to total due to rounding

STATISTICAL TABLES RELATED TO THE *PRIVACY ACT*

Table 1

Privacy Act dispositions of access and privacy complaints* by institution

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded resolved	ER-resolved	Total
Administrative Tribunals Support Service of Canada								1	1
Agriculture and Agri-food Canada								1	1
Bank of Canada								1	1
Canada Border Services Agency	4		2		2		3	36	47
Canada Mortgage and Housing Corporation			1						1
Canada Post Corporation	4					1		15	20
Canada Revenue Agency	8		13	1		1		31	54
Canada School of Public Service					1			1	2
Canadian Air Transport Security Authority								1	1
Canadian Broadcasting Corporation								1	1
Canadian Food Inspection Agency							1	5	6
Canadian Human Rights Commission							1	2	3
Canadian Human Rights Tribunal	1								1
Canadian Museum of History	1								1
Canadian Radio-television and Telecommunications Commission	1								1
Canadian Security Intelligence Service	1		9		1			20	31
Communications Security Establishment Canada			1					3	4
Correctional Service Canada	6		9	2	6	6	5	56	90
Department of Justice Canada			3		1		2	6	12
Department of National Defence	4		5	1	4	1		19	34
Elections Canada								1	1
Employment and Social Development Canada	4		5		1	1	1	14	26
Environment and Climate Change Canada			1	4					5
Financial Transaction and Reports Analysis Centre of Canada			1					2	3
Fisheries and Oceans Canada			1			1		1	3
Global Affairs Canada								1	1
Health Canada			1					4	5
Immigration and Refugee Board of Canada	2		1					4	7

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded resolved	ER-resolved	Total
Immigration, Refugees and Citizenship Canada	1		4		3			20	**28**
Indigenous and Northern Affairs Canada								5	**5**
Innovation, Science and Economic Development Canada	2							1	**3**
Library and Archives Canada								6	**6**
Marine Atlantic Inc.								1	**1**
National Energy Board								1	**1**
National Research Council of Canada					1			2	**3**
Natural Resources Canada			1	1		1		2	**5**
Office of the Commissioner of Official Languages							2		**2**
Office of the Correctional Investigator								2	**2**
Office of the Information Commissioner of Canada	1					2		1	**4**
Office of the Public Sector Integrity Commissioner of Canada								1	**1**
Parks Canada Agency				1				2	**3**
Parole Board of Canada	1		1			1	1	8	**12**
Privy Council Office			1			1	1	2	**5**
Public Health Agency of Canada								1	**1**
Public Safety Canada			2					2	**4**
Public Service Commission of Canada				1				6	**7**
Public Services and Procurement Canada	1					2	1	8	**12**
Royal Canadian Mounted Police	6	1	4		3	10	3	48	**75**
Security Intelligence Review Committee								1	**1**
Service Canada			1					3	**4**
Shared Services Canada								3	**3**
Statistics Canada	1							9	**10**
Sustainable Development Technology Canada			1						**1**
Transport Canada	2		1	1			1	6	**11**
Treasury Board of Canada Secretariat								1	**1**
Veterans Affairs Canada		2	4	1		2		10	**19**
Veterans Review and Appeal Board								1	**1**
VIA Rail Canada								2	**2**
Western Economic Diversification Canada								1	**1**
Total	**51**	**3**	**73**	**13**	**23**	**30**	**22**	**382**	**597**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 2

Privacy Act treatment times – Early resolution cases by complaint type*

Complaint type	Count	Average treatment time in months
Access	**221**	**3.54**
Access	214	3.57
Correction/notation	7	2.83
Privacy	**161**	**5.79**
Accuracy	2	6.58
Collection	21	7.71
Other	1	3.29
Retention and disposal	7	5.58
Use and disclosure	130	5.50
Time limits	**59**	**1.65**
Total	**441**	**4.11**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 3

Privacy Act treatment times – Standard investigations by complaint type*

Complaint type	Count	Average treatment time in months
Access	**124**	**20.86**
Access	120	20.98
Correction/notation	2	8.42
Language	2	25.63
Privacy	**91**	**23.41**
Accuracy	1	8.83
Collection	15	20.78
Retention and disposal	4	26.65
Use and disclosure	71	23.98
Time limits	**552**	**6.28**
Extension notice	25	3.32
Time limits	527	6.42
Total	**767**	**10.67**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 4

Privacy Act treatment times – All closed files by disposition*

Complaint type	Count	Average treatment time (months)
Standard investigations	**767**	**10.70**
Well-founded resolved	523	6.88
Not well-founded	86	18.04
Discontinued	86	16.44
Well-founded	31	27.29
Settled	23	23.81
Resolved	15	12.91
No jurisdiction	3	10.39
Early resolution - resolved	**441**	**4.11**
Total	**1208**	**8.30**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 5

Privacy Act breaches by institution

Respondent	Incident
Canada Border Services Agency	1
Canada Revenue Agency	25
Canadian Human Rights Commission	1
Canadian Radio-Television and Telecommunications Commission	1
Communications Security Establishment Canada	1
Correctional Service Canada	4
Department of Finance Canada	1
Department of Justice Canada	1
Employment and Social Development Canada	194
Fisheries and Oceans Canada	3
Global Affairs Canada	3
Health Canada	1
Immigration, Refugees and Citizenship Canada	7
Indigenous and Northern Affairs Canada	4
National Energy Board	1
Natural Resources Canada	1
Office of the Correctional Investigator	1
Public Safety Canada	1
Public Sector Pension Investment Board	1
Public Service Commission of Canada	6
Public Services and Procurement Canada	3
Revera Inc.	1
Royal Canadian Mint	1
Royal Canadian Mounted Police	12
Statistics Canada	3
Telefilm Canada	1
Transport Canada	2
Treasury Board of Canada Secretariat	2
Veterans Affairs Canada	2
VIA Rail Canada	1
Total	**286**

Table 6

Privacy Act complaints and breaches

Category	Total
Accepted	
Access	300
Privacy	256
Time limits	698
Total accepted	**1254**
Closed through early resolution	
Access	221
Privacy	161
Time limits	59
Total	**441**
Closed through standard investigation	
Access	124
Privacy	91
Time limits	552
Total	**767**
Total closed*	**1208**
Breaches received	
Accidental disclosure	83
Loss	178
Theft	3
Unauthorized access	22
Total received	**286**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 7

Privacy Act complaints accepted by complaint type

Complaint type	Early resolution		Investigation		Total count	Total percentage
	Count	Percentage	Count	Percentage		
Access						
Access	216	49%	75	9%	**291**	**23%**
Correction/notation	5	1%	3	0%	**8**	**1%**
Language	1	0%			**1**	**0%**
Privacy						
Accuracy	1	0%	2	0%	**3**	**0%**
Collection	18	4%	27	3%	**45**	**4%**
Other	1	0%			**1**	**0%**
Retention and disposal	7	2%	3	0%	**10**	**1%**
Use and disclosure	135	31%	62	8%	**197**	**16%**
Time limits						
Correction – time limits			1	0%	**1**	**0%**
Extension notice			15	2%	**15**	**1%**
Time limits	56	13%	626	77%	**682**	**54%**
Total*	**440**	**100%**	**814**	**100%**	**1254**	**100%**

* Figures may not sum to total due to rounding

Table 8

Privacy Act top 10 institutions by complaints accepted

Respondent	Access		Time limits		Privacy		Total
	Early resolution	Investigation	Early resolution	Investigation	Early resolution	Investigation	
Correctional Service Canada	27	18	33	7	24	331	**440**
Royal Canadian Mounted Police	16	14	37	22	12	131	**232**
Department of National Defence	7	3	14	3	7	59	**93**
Canada Border Services Agency	10	13	25	9	5	14	**76**
Canada Revenue Agency	20	7	18	2	1	15	**63**
Public Services and Procurement Canada	8	2	4	1	3	31	**49**
Canada Post Corporation	8	5	9	2		9	**33**
Immigration, Refugees and Citizenship Canada	9		4	3	3	10	**29**
Canadian Security Intelligence Service	1		15	4		6	**26**
Employment and Social Development Canada	7	2	7	5		3	**24**
Total	**113**	**64**	**166**	**58**	**55**	**609**	**1065**

Table 9

Privacy Act top 10 institutions in 2017–18 by complaints accepted and fiscal year

Respondent	2014-15	2015-16	2016-17	2017-18
Correctional Services Canada	314	547	389	440
Royal Canadian Mounted Police	140	120	160	232
Department of National Defence	68	77	146	93
Canada Border Services Agency	66	88	107	76
Canada Revenue Agency	106	85	65	63
Public Services and Procurement Canada	9	10	25	49
Canada Post Corporation	32	17	19	33
Immigration, Refugees and Citizenship	42	44	60	29
Canadian Security Intelligence Service	21	31	30	26
Employment and Social Development Canada	35	42	36	24
Total	**833**	**1061**	**1037**	**1065**

Table 10

Privacy Act complaints accepted by institution

Respondent	Early resolution	Investigation	Total
Administrative Tribunals Support Service of Canada	1	0	**1**
Agriculture and Agri-food Canada	1	0	**1**
Bank of Canada	1	0	**1**
Canada Border Services Agency	40	36	**76**
Canada Post Corporation	17	16	**33**
Canada Revenue Agency	39	24	**63**
Canada School of Public Service	1	0	**1**
Canadian Air Transport Security Authority	1	0	**1**
Canadian Broadcasting Corporation	3	1	**4**
Canadian Food Inspection Agency	5	1	**6**
Canadian Human Rights Commission	2	2	**4**
Canadian Radio-Television and Telecommunications Commission	3	1	**4**
Canadian Security Intelligence Service	16	10	**26**
Canadian Transportation Agency	1	0	**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	0	7	**7**
Communications Security Establishment Canada	3	1	**4**
Correctional Service Canada	84	356	**440**
Defence Construction Canada	0	1	**1**
Department of Justice Canada	9	6	**15**
Department of National Defence	28	65	**93**
Elections Canada	1	1	**2**
Employment and Social Development Canada	14	10	**24**
Environment and Climate Change Canada	0	1	**1**
Financial Transaction and Reports Analysis Centre of Canada	2	0	**2**
Fisheries and Oceans Canada	3	1	**4**
Global Affairs Canada	0	2	**2**
Health Canada	6	3	**9**
Immigration and Refugee Board of Canada	0	2	**2**
Immigration, Refugees and Citizenship Canada	16	13	**29**
Indigenous and Northern Affairs Canada	7	8	**15**
Innovation, Science and Economic Development Canada	2	3	**5**

Respondent	Early resolution	Investigation	Total
Library and Archives Canada	7	1	8
Marine Atlantic Inc.	1	0	1
National Energy Board	1	1	2
National Film Board of Canada	1	0	1
Natural Resources Canada	1	0	1
Office of the Correctional Investigator	2	0	2
Office of the Information Commissioner of Canada	1	0	1
Office of the Public Sector Integrity Commissioner of Canada	1	1	2
Parks Canada Agency	1	0	1
Parole Board of Canada	5	0	5
Privy Council Office	2	0	2
Public Health Agency of Canada	0	3	3
Public Prosecution Service of Canada	1	3	4
Public Safety Canada	3	0	3
Public Service Commission of Canada	1	1	2
Public Services and Procurement Canada	15	34	49
Quebec Port Authority	0	1	1
Royal Canadian Mounted Police	65	167	232
Security Intelligence Review Committee	1	0	1
Service Canada	3	2	5
Shared Services Canada	2	0	2
Statistics Canada	2	2	4
Status of Women Canada	4	0	4
Transport Canada	4	17	21
Treasury Board of Canada Secretariat	0	3	3
Veterans Affairs Canada	6	6	12
Veterans Review and Appeal Board	1	0	1
VIA Rail Canada	2	1	3
Western Economic Diversification Canada	1	0	1
Total	**440**	**814**	**1254**

Table 11

Privacy Act complaints accepted by province/territory/other

Province/territory/ other	Early resolution		Investigation		Total count	Total percentage
	Count	Percentage	Count	Percentage		
Alberta	53	12.05%	88	10.81%	**141**	**11.24%**
British Columbia	89	20.23%	221	27.15%	**310**	**24.72%**
Manitoba	16	3.64%	22	2.70%	**38**	**3.03%**
New Brunswick	20	4.55%	42	5.16%	**62**	**4.94%**
Newfoundland and Labrador	6	1.36%	10	1.23%	**16**	**1.28%**
Northwest Territories	1	0.23%	3	0.37%	**4**	**0.32%**
Nova Scotia	14	3.18%	25	3.07%	**39**	**3.11%**
Nunavut	3	0.68%	0	0.00%	**3**	**0.24%**
Ontario	164	37.27%	211	25.92%	**375**	**29.90%**
Prince Edward Island	2	0.45%	2	0.25%	**4**	**0.32%**
Quebec	60	13.64%	158	19.41%	**218**	**17.38%**
Saskatchewan	1	0.23%	21	2.58%	**22**	**1.75%**
Yukon	1	0.23%	1	0.12%	**2**	**0.16%**
Not specified	2	0.45%	5	0.61%	**7**	**0.56%**
Other (not U.S.)	7	1.59%	2	0.25%	**9**	**0.72%**
United States	1	0.23%	3	0.37%	**4**	**0.32%**
Total*	**440**	**100.00%**	**814**	**100.00%**	**1254**	**100.00%**

* Figures may not sum to total due to rounding

Table 12

Privacy Act dispositions by complaint type*

Complaint type	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded resolved	ER-resolved	Total
Access									
Access	29		46	9	9	5	22	214	**334**
Correction/ notation			1	1				7	**9**
Language					2				**2**
Privacy									
Accuracy			1					2	**3**
Collection	1		8	1	1	4		21	**36**
Other								1	**1**
Retention and disposal	2	1			1			7	**11**
Use and disclosure	19	2	17	2	10	21		130	**201**
Time limits									
Extension notice			4			1	20		**25**
Time limits	35		9	2			481	59	**586**
Total	**86**	**3**	**86**	**15**	**23**	**31**	**523**	**441**	**1208**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

Table 13

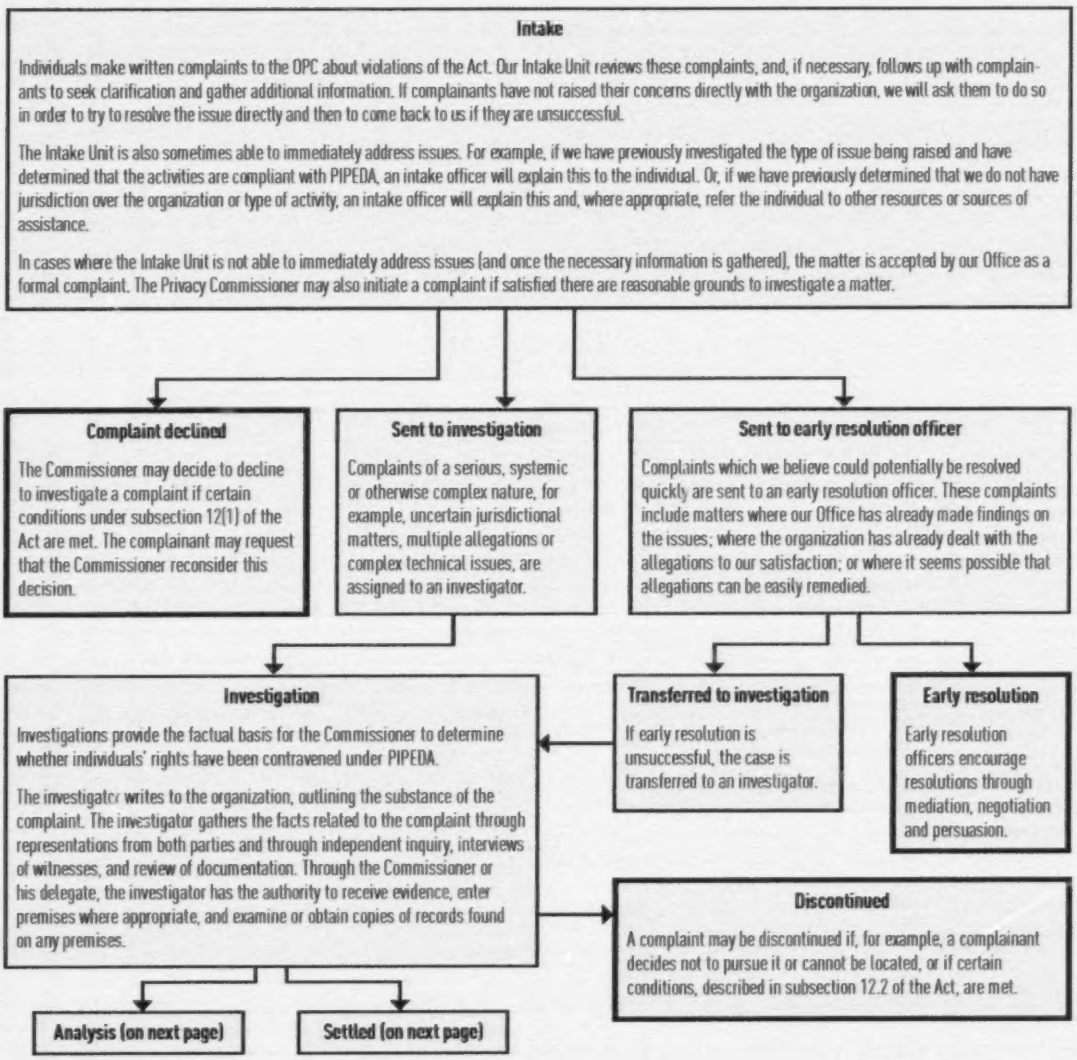
Privacy Act dispositions of time limits by institution*

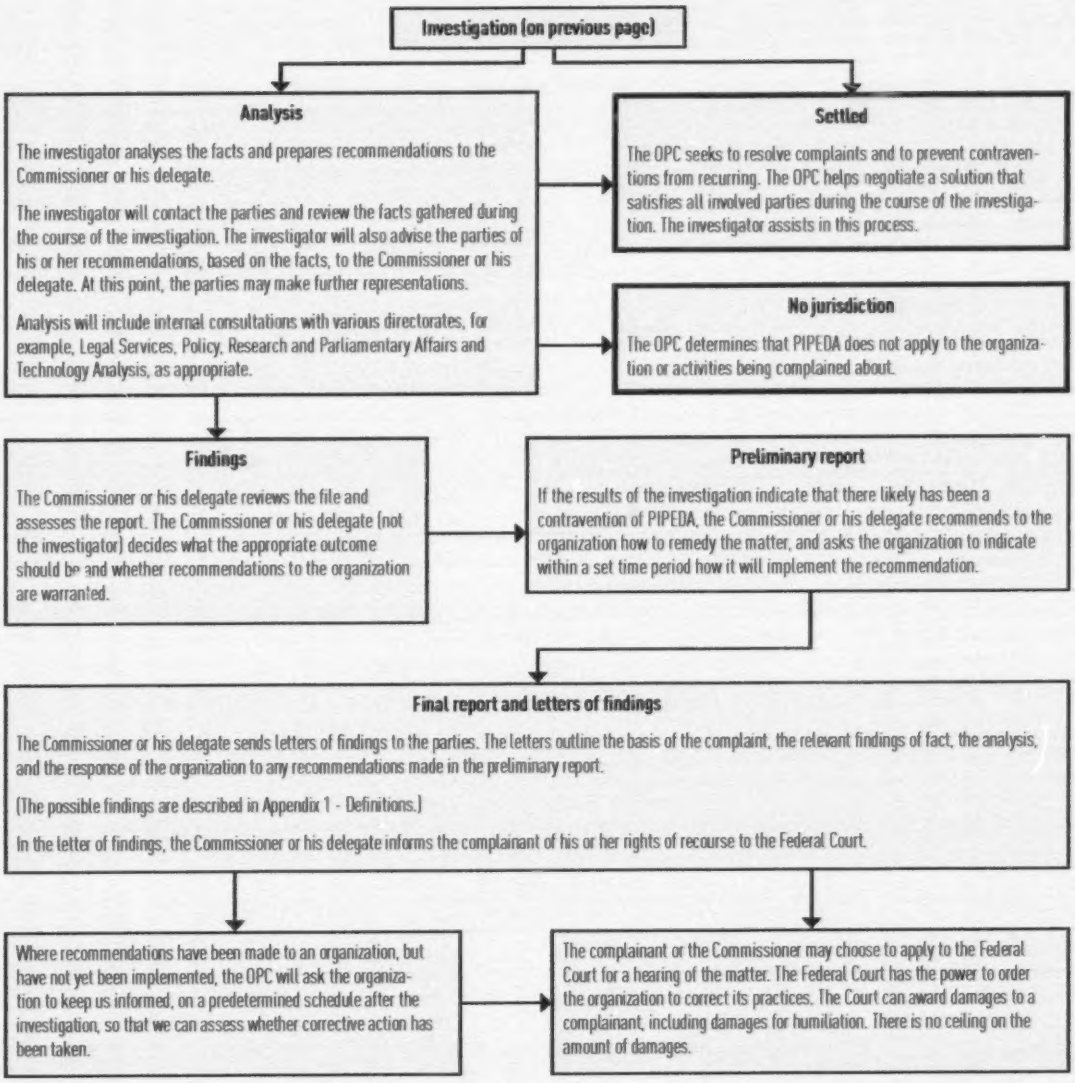
Respondent	Discontinued	Not well-founded	Resolved	Well-founded	Well-founded resolved	ER-resolved	Total
Canada Border Services Agency		2			26	5	**33**
Canada Post Corporation	2	1		1	3		**7**
Canada Revenue Agency					14	1	**15**
Canadian Human Rights Commission					1		**1**
Canadian Security Intelligence Service					3		**3**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police					1		**1**
Correctional Service Canada	27	1			253	24	**305**
Department of Justice Canada					3	1	**4**
Department of National Defence		3	1		44	7	**55**
Employment and Social Development Canada	2	1			5	3	**11**
Environment and Climate Change Canada					5		**5**
Global Affairs Canada					1		**1**
Health Canada					2		**2**
Immigration, Refugees and Citizenship Canada	2		1		8	3	**14**
Indigenous and Northern Affairs Canada					1		**1**
Innovation, Science and Economic Development Canada					2		**2**
Office of the Commissioner of Official Languages					1		**1**
Public Health Agency of Canada					1		**1**
Public Prosecution Service of Canada					1		**1**
Public Service Commission of Canada		1			1		**2**
Public Services and Procurement Canada		2			34	3	**39**
Royal Canadian Mounted Police	1	1			73	12	**87**
Service Canada					1		**1**
Transport Canada	1	1			13		**15**
Treasury Board of Canada Secretariat					1		**1**
Veterans Affairs Canada					3		**3**
Total	**35**	**13**	**2**	**1**	**501**	**59**	**611**

* PA complaints closed based on count of one for each series of complaints dealing with related issue; excluded complaints total 26

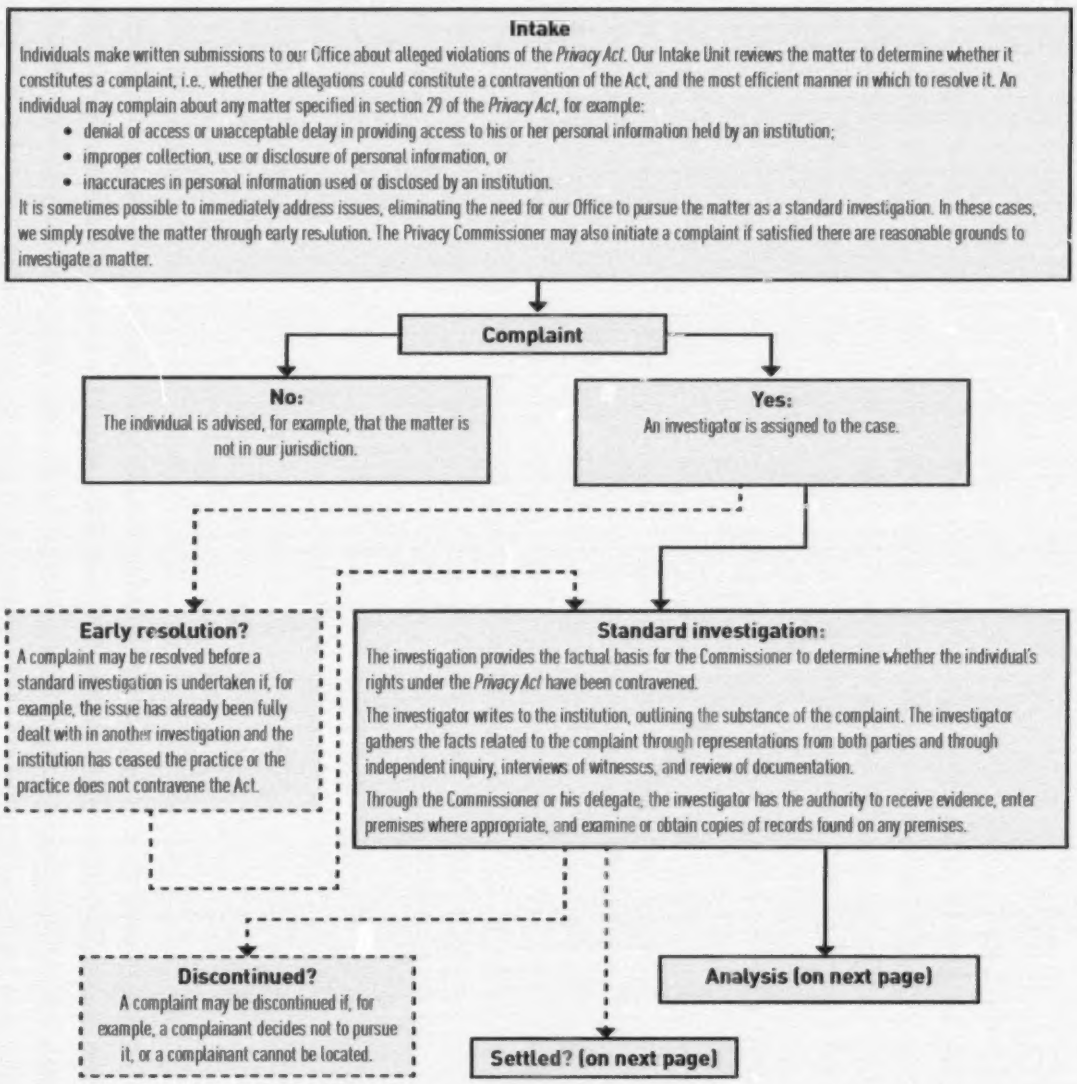
Appendix 3 – Investigation processes

PIPEDA INVESTIGATION PROCESS

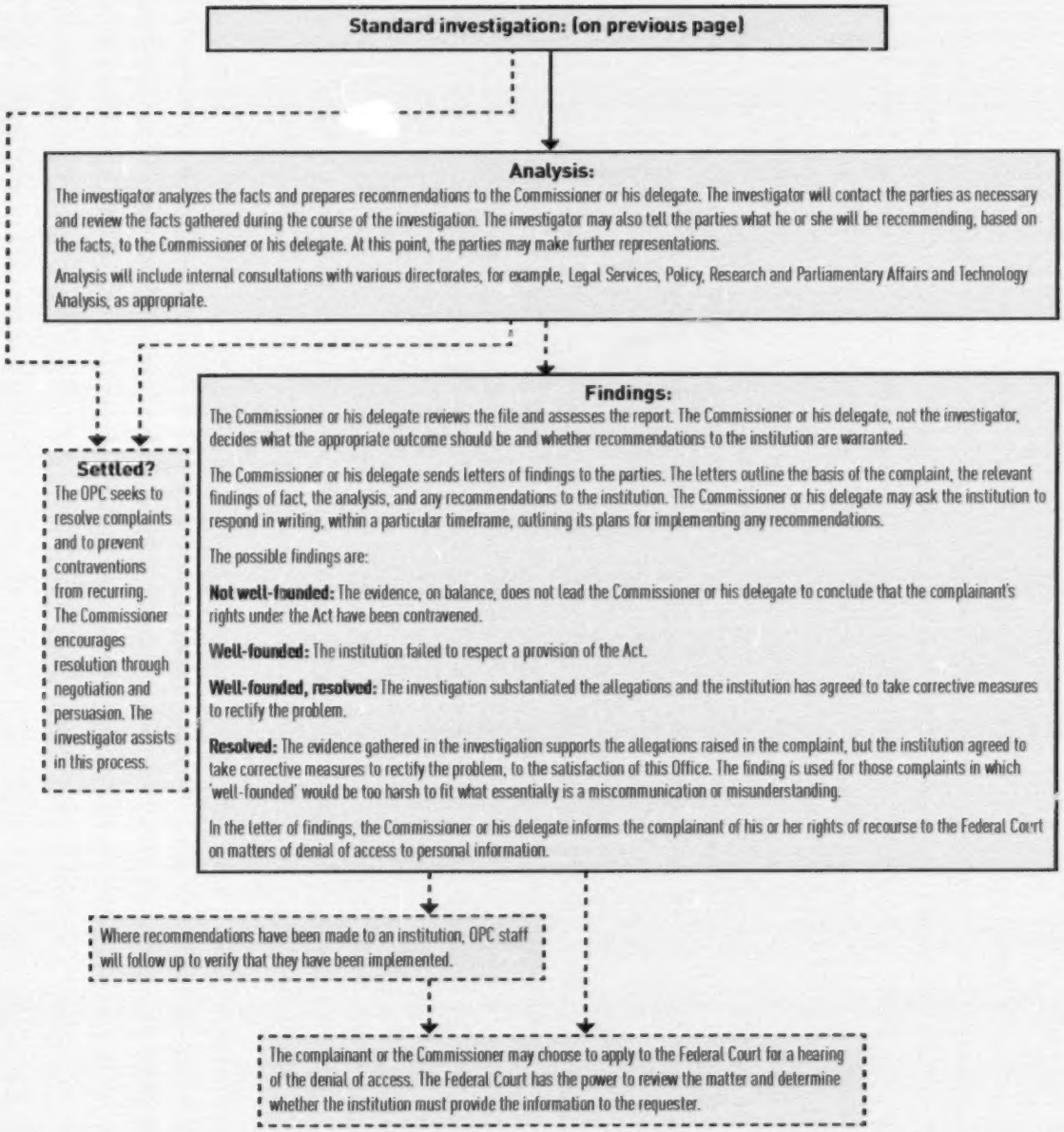

Intake
Individuals make written complaints to the OPC about violations of the Act. Our Intake Unit reviews these complaints, and, if necessary, follows up with complainants to seek clarification and gather additional information. If complainants have not raised their concerns directly with the organization, we will ask them to do so in order to try to resolve the issue directly and then to come back to us if they are unsuccessful.
The Intake Unit is also sometimes able to immediately address issues. For example, if we have previously investigated the type of issue being raised and have determined that the activities are compliant with PIPEDA, an intake officer will explain this to the individual. Or, if we have previously determined that we do not have jurisdiction over the organization or type of activity, an intake officer will explain this and, where appropriate, refer the individual to other resources or sources of assistance.
In cases where the Intake Unit is not able to immediately address issues (and once the necessary information is gathered), the matter is accepted by our Office as a formal complaint. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.
Complaint declined
The Commissioner may decide to decline to investigate a complaint if certain conditions under subsection 12(1) of the Act are met. The complainant may request that the Commissioner reconsider this decision.
Sent to investigation
Complaints of a serious, systemic or otherwise complex nature, for example, uncertain jurisdictional matters, multiple allegations or complex technical issues, are assigned to an investigator.
Sent to early resolution officer
Complaints which we believe could potentially be resolved quickly are sent to an early resolution officer. These complaints include matters where our Office has already made findings on the issues; where the organization has already dealt with the allegations to our satisfaction; or where it seems possible that allegations can be easily remedied.
Investigation
Investigations provide the factual basis for the Commissioner to determine whether individuals' rights have been contravened under PIPEDA.
The investigator writes to the organization, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Commissioner or his delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.
Transferred to investigation
If early resolution is unsuccessful, the case is transferred to an investigator.
Early resolution
Early resolution officers encourage resolutions through mediation, negotiation and persuasion.
Discontinued
A complaint may be discontinued if, for example, a complainant decides not to pursue it or cannot be located, or if certain conditions, described in subsection 12.2 of the Act, are met.
Analysis (on next page)
Settled (on next page)


Investigation (on previous page)
Analysis
The investigator analyses the facts and prepares recommendations to the Commissioner or his delegate.
The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also advise the parties of his or her recommendations, based on the facts, to the Commissioner or his delegate. At this point, the parties may make further representations.
Analysis will include internal consultations with various directorates, for example, Legal Services, Policy, Research and Parliamentary Affairs and Technology Analysis, as appropriate.
Settled
The OPC seeks to resolve complaints and to prevent contraventions from recurring. The OPC helps negotiate a solution that satisfies all involved parties during the course of the investigation. The investigator assists in this process.
No jurisdiction
The OPC determines that PIPEDA does not apply to the organization or activities being complained about.
Findings
The Commissioner or his delegate reviews the file and assesses the report. The Commissioner or his delegate (not the investigator) decides what the appropriate outcome should be and whether recommendations to the organization are warranted.
Preliminary report
If the results of the investigation indicate that there likely has been a contravention of PIPEDA, the Commissioner or his delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time period how it will implement the recommendation.
Final report and letters of findings
The Commissioner or his delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.
(The possible findings are described in Appendix 1 - Definitions.)
In the letter of findings, the Commissioner or his delegate informs the complainant of his or her rights of recourse to the Federal Court.
Where recommendations have been made to an organization, but have not yet been implemented, the OPC will ask the organization to keep us informed, on a predetermined schedule after the investigation, so that we can assess whether corrective action has been taken.
The complainant or the Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

PRIVACY ACT INVESTIGATION PROCESS


Intake
Individuals make written submissions to our Office about alleged violations of the Privacy Act. Our Intake Unit reviews the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act, and the most efficient manner in which to resolve it. An individual may complain about any matter specified in section 29 of the Privacy Act, for example:
• denial of access or unacceptable delay in providing access to his or her personal information held by an institution;
• improper collection, use or disclosure of personal information, or
• inaccuracies in personal information used or disclosed by an institution.
It is sometimes possible to immediately address issues, eliminating the need for our Office to pursue the matter as a standard investigation. In these cases, we simply resolve the matter through early resolution. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.
Complaint
No:
The individual is advised, for example, that the matter is not in our jurisdiction.
Yes:
An investigator is assigned to the case.
Early resolution?
A complaint may be resolved before a standard investigation is undertaken if, for example, the issue has already been fully dealt with in another investigation and the institution has ceased the practice or the practice does not contravene the Act.
Standard investigation:
The investigation provides the factual basis for the Commissioner to determine whether the individual's rights under the Privacy Act have been contravened.
The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation.
Through the Commissioner or his delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.
Discontinued?
A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.
Analysis (on next page)
Settled? (on next page)

Note: a broken line (- - - -) indicates a *possible* outcome.


Standard investigation: (on previous page)
Analysis:
The investigator analyzes the facts and prepares recommendations to the Commissioner or his delegate. The investigator will contact the parties as necessary and review the facts gathered during the course of the investigation. The investigator may also tell the parties what he or she will be recommending, based on the facts, to the Commissioner or his delegate. At this point, the parties may make further representations.
Analysis will include internal consultations with various directorates, for example, Legal Services, Policy, Research and Parliamentary Affairs and Technology Analysis, as appropriate.
Settled?
The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through negotiation and persuasion. The investigator assists in this process.
Findings:
The Commissioner or his delegate reviews the file and assesses the report. The Commissioner or his delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.
The Commissioner or his delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Commissioner or his delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.
The possible findings are:
Not well-founded: The evidence, on balance, does not lead the Commissioner or his delegate to conclude that the complainant's rights under the Act have been contravened.
Well-founded: The institution failed to respect a provision of the Act.
Well-founded, resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.
Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which 'well-founded' would be too harsh to fit what essentially is a miscommunication or misunderstanding.
In the letter of findings, the Commissioner or his delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.
Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.
The complainant or the Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Note: a broken line (- - -) indicates a *possible* outcome.

Appendix 4 – Report of the Privacy Commissioner, Ad Hoc, for 2017–18

It is my pleasure to report here on the activities of the Office of the Privacy Commissioner, Ad Hoc. On April 1, 2007, the Office of the Privacy Commissioner (OPC) became subject to the *Privacy Act* (Act). This means that a privacy request can be made to the OPC as an institution to which the right of access to personal information applies.

The law that brought this about did not, however, create a mechanism separate from the OPC, which oversees government compliance with privacy requests, to investigate any complaints that privacy requests to the OPC have not been handled as the Act requires.

Since it is a fundamental principle of the privacy law that decisions on the disclosure of government information should be reviewed independently, the office of an independent Privacy Commissioner Ad Hoc was created and given the authority to investigate any such complaints about the OPC.

The Privacy Commissioner has delegated the majority of his powers, duties and functions to me as set out in sections 29 through 35 and section 42 of the Act in order that I can investigate *Privacy Act* complaints lodged against the OPC.

Outstanding complaints from previous year

Our office had no outstanding complaints from the previous year.

New complaints this year

Two complaints were received this year; all were investigated and disposed of by the end of fiscal year.

The issue of the first complaint was a refusal of access. The OPC had responded to the requester that all records had already been provided to him in a previous privacy request. Unsatisfied with this response, the complainant alleged that the OPC failed to conduct a comprehensive search and that more new records ought to exist.

My investigation concluded that the OPC had in fact provided all the responsive records in a previous request submitted by the complainant and that no new additional information existed. I therefore found this complaint to be not-well-founded.

The second complaint concerned the application of paragraph 22.1(1) of the Act. This paragraph exempts from production information obtained or created in the course of an investigation by the OPC. Once the investigation and all related proceedings are finally concluded, however, the exemption is partially lifted. At that point, the exemption no longer applies to documents created during the investigation.

My investigation revealed that the disputed documents had been obtained during the course of the OPC's own investigations. I therefore found that the OPC properly applied the mandatory exemption in refusing to disclose the requested documents. This complaint was not-well-founded.

In addition to these two complaints, this Office also received correspondence from a number of individuals who were dissatisfied with how the OPC had investigated their underlying complaint, or had not been timely, in their view, in responding to their complaints.

This Office does not have jurisdiction to investigate concerns about how the OPC has investigated complaints made to it as the oversight body under the Act. Nor can my Office investigate concerns about delay by the OPC in processing such complaints. My mandate is limited to receiving and investigating complaints that an access request for a record under the control of the OPC itself may have been improperly handled.

Conclusion

The existence of an independent Commissioner, Ad Hoc, helps to ensure the integrity of the OPC's handling of privacy access requests made to it, as an institution, and therefore contributes to the overall system of access to information at the federal level. My Office looks forward to continuing to play this part in access to information.

David Loukidelis QC
Commissioner, Ad Hoc for the
Office of the Privacy Commissioner of Canada

March 2018